NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

WHISTLEBLOWING IN A WIKILEAKS WORLD: A MODEL FOR RESPONSIBLE DISCLOSURE IN HOMELAND SECURITY

by

Gregory M. Bernard

March 2012

Thesis Co-Advisors: Rodrigo Nieto-Gomez
John Rollins

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE *Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE March 2012

3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Whistleblowing in a Wikileaks World: A Model for Responsible Disclosure in Homeland Security

5. FUNDING NUMBERS

6. AUTHOR(S) Gregory M. Bernard

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ________N/A________.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Whistleblowing serves as a check/balance system to the government bureaucracy, helping to bypass administrative roadblocks and to provide a mechanism through which homeland security can monitor and increase efficiency in its operations. However, homeland security also deals with information that can be of a sensitive or secret nature, the unauthorized disclosure of which can cause damage to both homeland security efforts and national security. The current process for the authorized submission of whistleblowing information fails to provide whistleblowers the protections they require, instead encouraging whistleblowers to disclose information to the media or through stateless news organizations like Wikileaks to prevent reprisals.

The technological capability to provide whistleblowers protections through anonymity currently exists, and has been demonstrated to be effective. By leveraging those technologies and setting up an authorized process for responsible disclosure, through which homeland security employees can submit whistleblowing information without fear of reprisals, it may increase the likelihood of whistleblowers reporting issues in the first place, and reduce the number of leaks to unauthorized recipients (media/stateless news organizations).

14. SUBJECT TERMS Whistleblowing, Wikileaks, Responsible Disclosure, Anonymity, Homeland Security, Overclassification, Information Sharing, Public Trust, Government, Bureaucracy, Transparency, Secrecy, Fraud, Waste, Abuse, Organizational Misconduct, Protection, Retaliation, Reprisal, Technology

15. NUMBER OF PAGES
145

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

THIS PAGE INTENTIONALLY LEFT BLANK

WHISTLEBLOWING IN A WIKILEAKS WORLD: A MODEL FOR RESPONSIBLE DISCLOSURE IN HOMELAND SECURITY

Gregory M. Bernard
Branch Chief, Domestic Nuclear Detection Office
U.S. Department of Homeland Security, Washington, DC
B.A., University of Maryland, 2003

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2012**

Author: Gregory M. Bernard

Approved by: Rodrigo Nieto-Gomez
Thesis Co-Advisor

John Rollins
Thesis Co-Advisor

Daniel Moran, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Whistleblowing serves as a check/balance system to the government bureaucracy, helping to bypass administrative roadblocks and to provide a mechanism through which homeland security can monitor and increase efficiency in its operations. However, homeland security also deals with information that can be of a sensitive or secret nature, the unauthorized disclosure of which can cause damage to both homeland security efforts and national security. The current process for the authorized submission of whistleblowing information fails to provide whistleblowers the protections they require, instead encouraging whistleblowers to disclose information to the media or through stateless news organizations like Wikileaks to prevent reprisals.

The technological capability to provide whistleblowers protections through anonymity currently exists, and has been demonstrated to be effective. By leveraging those technologies and setting up an authorized process for responsible disclosure, through which homeland security employees can submit whistleblowing information without fear of reprisals, it may increase the likelihood of whistleblowers reporting issues in the first place, and reduce the number of leaks to unauthorized recipients (media/stateless news organizations).

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AFGE	American Federation of Government Employees
CSRA	Civil Service Reform Act
DHS	Department of Homeland Security
DoD	Department of Defense
E.O.	Executive Order
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GAP	Government Accountability Project
HSDN	Homeland Secure Data Network
IC	Intelligence Community
IG	Inspector General
JWICS	Joint Worldwide Intelligence Communications System
MITM	Man-in-the-middle
MSPB	Merit Systems Protection Board
NGO	Non-Governmental Organization
NSA	National Security Agency
NTP	Neutral Trusted Party
OSC	Office of Special Counsel
PIDA	Public Information Disclosures Act
POGO	Project on Government Oversight
RDIS	Responsible Disclosure Information System
SIPRNET	Secure Internet Protocol Router Network
SOPA	Stop Online Piracy Act
TOR	The Onion Router

UK	United Kingdom
VPN	Virtual Private Network
WPA	Whistleblower Protection Act
WPEA	Whistleblower Protection Enhancement Act
WWTW	Whistling While They Work

EXECUTIVE SUMMARY

Introduction—A dramatic change in the information-sharing environment has occurred over the last decade. New technologies, the rapid evolution of the Internet, and innovations in social media have provided the ability to gather and share information at an unprecedented level. The Executive Branch of the U.S. Government touts the virtues of transparency, while Congress defines whistleblowing and the disclosure of government fraud/waste/abuse as a "civic duty", and yet the Freedom of Information Act (FOIA) process is broken, the Whistleblower Protection Act (WPA) is woefully inadequate, and secrecy continues to run rampant. The disclosure of hundreds of thousands of potentially classified documents to the organization Wikileaks may be an example of what this contradiction has caused. The existence of Wikileaks as an organization is irrelevant now, and their most significant contribution is not the release of 1.2 million documents. Rather, the most significant impact of Wikileaks is their successful demonstration and validation of the 'Wikileaks model.' Wikileaks has demonstrated the power of the Internet using web technologies to provide protections through anonymity, while giving individuals access to a worldwide audience. The current troubles faced by the organization may or may not portend the end of Wikileaks; however, it does provide a glimpse into the future of whistleblowing. Building upon the apparent success of the Wikileaks model, the *Wall Street Journal* and Al-Jazeera have both implemented "anonymous" whistleblower submission sites. This new paradigm for communications, as enabled by the innovative uses of the Internet and social media, provides both opportunities and areas for concern regarding government transparency.

Problem Statement—Whistleblowing serves as a critical check and balance system to government bureaucracy, helping to circumvent administrative roadblocks and to provide a mechanism through which homeland security can monitor and increase efficiency in its operations. Homeland security also deals with information that can be of a sensitive or secret nature, the unauthorized disclosure of which can cause damage to both homeland security efforts and national security. Maintaining the balance between secrecy and transparency is a difficult proposition; however, current government efforts, particularly its handling of whistleblowers, places that balance in jeopardy. The government has taken some steps to address some of these problems; however, the government has also taken extreme measures to prosecute any whistleblowers who stray outside the appropriate submission process (i.e., deemed an unauthorized leak of sensitive/classified information) or are not protected by the WPA. Instead of acknowledging that current policy on whistleblowers is broken, the government's current course of action decreases the likelihood important fraud/waste/abuse information will be received from whistleblowers, while possibly influencing their decision and encouraging them to bypass authorized channels and instead utilize the Internet to protect themselves from identification and retaliation. The current lack of public trust in government, and the existence of alternative avenues for disclosure that provide greater protections than those currently offered by the U.S. Government, serve to exacerbate the problem.

Research Question—What policy model and associated technological process could the U.S. DHS implement that will encourage whistleblowers to submit information through authorized channels as opposed to leaking information to unauthorized parties?

Analysis—To answer the research question, this thesis explores three primary areas. The first is the whistleblowing environment, to include definitions, applicable policies, laws (both domestic and international), authorized and unauthorized processes, motivations, public trust, requirements, and intentions of all parties involved. The second area of focus is technology, specifically, the available options, best practices, and vulnerabilities of potential technological solutions (e.g., phone, email, web). The final portion of thesis serves to develop and evaluate policy options based on the findings and conclusions identified in the first two areas of analysis. Those findings are as follows.

- Overclassification is a problem
- Information sharing is critical to both U.S. security and U.S democracy
- Homeland security efforts require public (to include its employees and partners) trust and support to succeed
- The ability to keep secrets and maintain control of classified information will continue to decrease
- Decreasing overclassification will save the United States money
- Whistleblowing is a civic duty

- The government is committed to providing whistleblower protections
- Whistleblowers are in large part motivated by patriotism
- Anonymity is a positive incentive for whistleblowers
- Fourth and Fifth Estates (media and stateless news organizations) provide alternatives to the government process
- Public trust in the government has declined
- Public trust can be increased through the use of third parties
- Technology exists to provide anonymity to whistleblowers
- Current options for whistleblowing are inadequate

These premises form the foundation and justification for the implementation of any solution.

Current legitimate/authorized processes, such as submission through standard government channels, present significant risks to the whistleblower. Clandestine/unauthorized processes, such as the Internet (Wikileaks) and mainstream media, represent a clear breach of the law, which is in conflict with the "do the right thing" mindset of many whistleblowers. If whistleblowers had a way to communicate identified issues through an authorized third party that would serve as a proxy on their behalf, it would undermine the current processes (both legitimate and clandestine), potentially making them obsolete. It would reduce the personal risk faced by whistleblowers by providing the anonymity that makes the clandestine approach attractive, without clearly breaking the law. The Department of Homeland Security has an opportunity to build upon and improve the "Wikileaks Model," to harness its use of technology and process to create a solution that would meet the needs of both whistleblowers and the government. If implemented correctly, the number of legitimate whistleblower complaints would increase (overall submissions would increase), and the number of whistleblowers who choose unauthorized avenues would be expected to decrease.

Recommendation—For any solution to be considered successful, it is critical to establish a clear definition of success. This thesis proposes the following definition of success for any whistleblowing solution.

> To promote the voluntary disclosure of information by any man or woman who reasonably believes that organizational wrongdoing has occurred, the facilitation of corrective action to address the wrongdoing, and providing for the protection of the submitter while maintaining information security, all within the bounds of U.S. law.

Four key pillars create the foundation for success.

- Whistleblowers must have the support of leadership
- Legislation and policies must be clear and straightforward
- Whistleblowing policies must enforce accountability
- Authorized channels must provide at least as much protection as unauthorized channels

The conclusions drawn in this thesis, including the policy model ultimately recommended, is based on the research and the findings identified above. Combined with a current understanding of the problem, the evaluation criteria, and the potential solutions available, it is recommended that the government establish a partnership with a non-government organization (NGO) within U.S. legal jurisdiction, and subsidize the establishment of a government sponsored whistleblower submission website and virtual private network. This solution would allow whistleblowers to submit information to the government with the protection of anonymity, through the third party NGO. Establishing this policy provides whistleblowers who truly believe in improving government operations through the submission of information on fraud/waste/abuse or other types of concerns, a legitimate way to achieve their goal without risking their career and future on the weak whistleblower protections currently in place. While it may not completely eliminate leaks to the media or organizations, such as Wikileaks, the researcher believes those leaks will decrease as more whistleblowers give the government an opportunity to act on their submission.

ACKNOWLEDGMENTS

This thesis would not have been possible without the contribution and support of many people. I cannot possibly express the full extent of my gratitude and appreciation, but I wish to acknowledge those who made it possible for me to complete this tremendous undertaking.

To my parents: Thank you very much for constantly pushing me to pursue additional opportunities for education and intellectual growth. Thank you also for the hours you spent reading and commenting on this thesis.

To my sister: Thank you for opening your world of educational resources and research expertise to me. Your support and encouragement helped to keep me motivated throughout this process.

To my friends and colleagues: Thank you for your understanding and support of the task I had to complete. Thank you also for reminding me that mental and physical breaks are necessary.

To the U.S. Department of Homeland Security: Thank you for supporting my participation in this program. Having the opportunity to engage in some of the most productive and educational dialogues and interactions through the Center for Homeland Defense and Security has granted me powerful perspectives on the issues facing our nation.

To the Naval Postgraduate School's Center for Homeland Defense and Security: Thank you for the opportunity to participate in cohorts 1005/1006. I know I was the Vincent Gambini of grad school applicants, but the opportunity afforded me through this program has truly been life changing. My only hope is that I was able to contribute as much as I received.

To the professors and staff of CHDS: Thank you for challenging me, pushing me to overcome any obstacles, and for motivating me to explore possibilities I had not considered. This thesis reflects input from every one of you, and without you, it would not have been possible.

To my beautiful fiancé: Thank you for supporting me during the last 18 months: for tolerating my books and papers all over the house, bearing with my rants on seemingly random topics, for being flexible and understanding when I waited until the last minute to finish an assignment, and most of all, for just being yourself, my inspiration.

I. INTRODUCTION

In February of 1777, just months after our founding fathers signed the Declaration of Independence, 10 sailors who had joined the U.S. Navy to fight for independence from Great Britain, met on board the warship *Warren.* They met, not to plan a battle against the King's armies, but rather to vet their concerns about the incompetence and lack of moral integrity of the commander in chief of the Continental Navy, Commodore Esek Hopkins. These sailors were devoted to fighting and winning the War for Independence. They were revolutionaries, risking their lives to build a free and independent America; they wanted nothing more than to fight and defeat their British foes. However, they feared that their commander could not successfully lead them. They blew the whistle on his mistreatment of prisoners, petitioning the Continental Congress and stating Hopkins had "treated prisoners in the most inhuman and barbarous manner." Congress acted on the information they received and removed Hopkins from office. Unfortunately, the incident did not end there. Hopkins had not only held the top Navy job, but also came from a powerful colonial family; his brother was governor of Rhode Island and one of the original signers of the Declaration of Independence. Hopkins sought revenge against the whistleblowers—retaliating against them both during his short remaining tenure as commander and after he was stripped of his command. On July 30, 1778, the Continental Congress came to the whistleblowers defense (Kohn, 2011).

Subsequently, the Continental Congress, without any recorded dissent, passed a resolution that encouraged all citizens to blow the whistle on official misconduct. It read:

> That it is the duty of all persons in the service of the United States, as well as all other inhabitants thereof, to give the earliest information to Congress or any other proper authority of any misconduct, frauds or misdemeanors committed by any officers or persons in the services of these states, which may come to their knowledge. (Continental Congress, 1778)

Whistleblowers have played a key role in government affairs since the founding fathers, facing significant personal risks of reprisals and retaliation to perform their patriotic duty to ensure the nation's safety and security. In the 236 years since then, and despite the best efforts of Congress, those risks remain.

A. PROBLEM STATEMENT

A dramatic change in the information-sharing environment has occurred over the last decade. New technologies, the rapid evolution of the Internet, and innovations in social media have provided the ability to gather and share information at an unprecedented level. The government's failure to adapt to the new environment and adequately address its over-classification problem (Hall, 2005), combined with a decline in investigative journalism and traditional news media's increasing inability to serve as a government watchdog, has created a public backlash, which is a particularly important issue for the Department of Homeland Security (DHS). The homeland security enterprise is comprised of "Federal, State, local tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population" (U.S. Department of Homeland Security, 2010). From suspicious activity reporting and contributing to the deterrence of terrorist activities, to leveraging public preparedness to empower communities, help minimize fear, and diminish the effectiveness of terrorist tactics, the public plays a key role in homeland security efforts (U.S. Department of Homeland Security, 2010). The Final Report of the National Commission on Terrorist Attacks Upon the United States (National Commision On Terrorist Attacks Upon The United States, 2004) found that existing trends of over-classification and secrecy deprived intelligence and law enforcement of a potent weapon against terrorism: an alert and well-informed American public (National Commision On Terrorist Attacks Upon The United States, 2004). Over-classification and the accompanying lack of transparency have eroded public trust in the government, resulting in a decrease in security as well.

The Executive Branch of the U.S. Government touts the virtues of transparency, while Congress defines whistleblowing and the disclosure of government fraud/waste/abuse as a “civic duty” (Committee on Government Reform, House of Representatives, 2006), and yet the Freedom of Information Act (FOIA) process is broken (U.S. Office of Special Counsel, 2004), the Whistleblower Protection Act (WPA) is woefully inadequate (Mihm, 2001), and secrecy continues to run rampant (Aftergood, 2010a). The disclosure of hundreds of thousands of potentially classified documents to the organization Wikileaks may be an example of what this contradiction has caused. While the majority of the U.S. Government and much of the news media had immediately condemned the website, describing the disclosure as treasonous and calling for the termination of the site itself and prosecution of its founder, Julian Assange; the fact remains that the situation has changed. The existence of Wikileaks as an organization is irrelevant now, and their most significant contribution is not the release of 1.2 million potentially classified documents. Rather, the most significant impact of Wikileaks is their successful demonstration and validation of the ‘Wikileaks model.’ Wikileaks has demonstrated the power of the internet using web technologies to provide protections through anonymity, while giving individuals access to a worldwide audience. The current troubles faced by the organization may or may not portend the end of Wikileaks as an organization; however, it does provide a glimpse into the future of whistleblowing. Building upon the apparent success of the Wikileaks model, the *Wall Street Journal* and Al-Jazeera have both implemented “anonymous” whistleblower submission sites. This new paradigm for communications, as enabled by the innovative uses of the Internet and social media, provides both opportunities and areas for concern regarding government transparency. It is time for a significant change in thinking regarding how the U.S. Government handles government whistleblowers.

Whistleblowing serves as a critical check and balance system to government bureaucracy, helping to circumvent administrative roadblocks and to provide a mechanism through which homeland security can monitor and increase efficiency in its operations. Two former federal agents have even made the case that 9/11 could have been prevented if whistleblowers had been able to bypass the key officials who ignored the warnings and prevented the sharing of key intelligence (Rowley, 2010). Even the 9/11 Commission concluded that had the information about Moussaouui's arrest been made public, the 9/11 plot may have been postponed (National Commision On Terrorist Attacks Upon The United States, 2004).

Homeland security deals with information that can be of a sensitive or secret nature, the unauthorized disclosure of which can cause damage to both homeland security efforts and national security. Maintaining the balance between secrecy and transparency is a difficult proposition; however, current government efforts, particularly its handling of whistleblowers, places that balance in jeopardy. The government has taken steps to address some of these problems by releasing new executive orders (E.O.) on classified information (Office of the White House Press Secretary, 2009), and new policies addressing some of the issues associated with FOIA (O'Keefe, 2009). The government has also taken extreme measures to prosecute any whistleblowers who stray outside the appropriate submission process (i.e., deemed an unauthorized leak of sensitive/classified information) or are not protected by the WPA (Goodman, 2007)). The government's position on whistleblowers is further confused by the recent anonymous hold placed on the passage of the Whistleblower Protection Enhancement Act (a measure designed to fix the issues with the WPA) in Congress, despite its bi-partisan support (S. Devine, 2010). Instead of acknowledging that current policy on whistleblowers is broken, the government's current course of action decreases the likelihood important fraud/waste/abuse information will be received from whistleblowers, while possibly influencing their decision and encouraging them to bypass authorized channels and instead utilize the Internet to protect themselves from identification and retaliation.

Despite widespread agreement that whistleblowers play an important role in government, current U.S. policies governing whistleblowers and their legal rights are widely accepted as inadequate, incomplete, and confusing. No fewer than fifteen separate laws provide some guidance on the authorized conduct for and the protection of whistleblowers. Worse still, even fewer protections exist for employees of "national security" agencies and the intelligence community (IC) which, remarkably, are not currently covered by the most significant legislation to date, the Whistleblower Protection Act. Despite repeated attempts by Congress to revise legislation and increase support of whistleblowers, the increase in unauthorized disclosures continues. The current lack of public trust in government, and the existence of alternative avenues for disclosure that provide greater protections than those currently offered by the U.S. Government, serve to exacerbate the problem.

B. RESEARCH QUESTION

What policy model and associated technological process could the U.S. DHS implement that will encourage whistleblowers to submit information through authorized channels as opposed to leaking information to unauthorized parties?

C. SIGNIFICANCE OF RESEARCH

This research is designed to identify a near-term implementable solution for the federal members of the homeland security enterprise to facilitate and increase authorized whistleblowing by providing whistleblower protections while simultaneously protecting sensitive information. While the primary consumer of this information will be the U.S. DHS and its partners, this solution will have broader applicability for other federal government entities, and state and local organizations as well. The policy, particularly its technological components, may have applications beyond whistleblowers as it could potentially be useful as an anonymous tip line for the public, encouraging participation in the national "See Something/Say Something" campaign. As is common with Web 2.0, the true value of technology only becomes apparent through its innovative application and use.

D. METHOD

To answer the research question, the researcher will employ a hybrid methodology including both conceptual modeling and policy analysis. This process consists of three primary steps.

The development of a conceptual model, which identifies and dissects the pieces, parts, and components of the whistleblowing environment to include applicable policies, laws, motivations, requirements, and intentions of all parties involved. This step will allow identification of these elements and determine findings and conclusions associated with each element.

The conduct of a technology evaluation, which defines the vulnerabilities of potential technological solutions. Clearly defining the vulnerabilities of information sharing systems (e.g., phone, email, web) will allow the best suited technology component(s) for the recommended policy to be identified.

The development of a recommended course of action (policy model) through a policy analysis based on the findings and conclusions identified by the conceptual model and the vulnerabilities identified through the technology evaluation. The policies will then be assessed against identified evaluation criteria.

E. HYPOTHESES OR TENTATIVE SOLUTIONS

Whistleblowing serves as a check/balance system to the government bureaucracy, helping to bypass administrative roadblocks and to provide a mechanism through which homeland security can monitor and increase efficiency in its operations. However, homeland security also deals with information that can be of a sensitive or secret nature, the unauthorized disclosure of which can cause damage to both homeland security efforts and national security. The current process for the authorized submission of whistleblowing information is broken, with current whistleblower policies providing protections only after reprisals or retaliation have occurred. The technological capability to provide whistleblowers protections through anonymity currently exists, and has been demonstrated to be effective. The concept of ‘Responsible Disclosure’ in the information security world is an excellent example of how critical vulnerability disclosures can be, and could serve as a model for a potential solution. By leveraging those technologies and creating an authorized process through which homeland security employees can submit whistleblowing information without fear of reprisals, it may increase the likelihood of whistleblowers reporting issues in the first place, and reduce the number of leaks to unauthorized recipients (media/stateless news organizations). While technological and policy solutions exist that can be applied to this problem by the government, the reality is any government solution is likely to be ineffective without addressing the issue of trust in some way.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. LITERATURE REVIEW

This literature review examines the body of knowledge on how the U.S. Government might leverage Internet technologies in balancing secrecy and transparency. The literature cites studies and previous works going back as far as the 1960s; yet much has happened over the last decade to shape the debate about secrecy/transparency in government affairs radically. Between the relatively recent adoption of the Internet into mainstream life and the renewed security concerns associated with the 'War on Terrorism,' the relevant literature identified in this thesis was primarily published after 2001. The sources have been derived from academic journals, mainstream media, non-governmental organizations (NGOs), and government reports, and are divided into three categories.

- E-Government Initiatives
- Internet Anonymity
- Government Secrecy and Whistleblowers

The approach each individual researcher takes varies greatly; however, their arguments are for the most part, mutually confirmatory. The one area with the largest disparity of conclusions is in the area of internet anonymity, while the conclusions on E-Government initiatives and government secrecy and whistleblowers are largely uniform. A few areas lack research and study, and those areas are identified as follows. It is significant to note that in a comparison of the recommendations identified in government reports, academic journals, and NGO reports, little discernible disagreement occurs.

1. E-Government Initiatives

E-Government has been defined as "the delivery of [government] information and services online via the Internet or other digitals means…and may include opportunities for online political participation" (Tolbert, 2006). The literature, which evaluates E-Government initiatives, has generally concluded the following: our nation's efforts, particularly homeland security, are dependent upon public trust and participation; E-

Government initiatives are designed to improve public confidence in government, and Web 2.0 has demonstrated particular use for government to both provide and receive information from the public.

While few agreed upon definitions of public trust exist, it is generally accepted across the literature that public trust and confidence play a key role in U.S. activities, and that it has declined significantly during the past decade (Welch, 2003; Moon, 2003; Tolbert, 2006; Banisar, 2007). Government reports have consistently recommended increased public engagement. The U.S. DHS in particular has increased its effort to include the public in the homeland security enterprise, specifically identifying the actions the public can take in the department’s Quadrennial Homeland Security Report. “From suspicious activity reporting and contributing to the deterrence of terrorist activities, to leveraging public preparedness to empower communities, help minimize fear, and diminish the effectiveness of terrorist tactics, the public plays a key role in homeland security efforts” (U.S. Department of Homeland Security, 2010).

The majority of the literature on E-Government initiatives describes their potential benefits in terms of positive gain in public confidence. By exploring case studies, scholars have evaluated the public response to E-Government initiatives, cost savings, and long term potential of these efforts to improve government efficiency and response time (West, 2004). Overall, agreement exists that E-Government initiatives show promise in providing significant benefits in each of those categories. Some concerns have arisen that efficiency gains with E-Government will beget a decline in quality, creating a “screen bureaucracy” that will actually increase distance between the public and the government. Also discussed is the point that while E-Government does provide marked improvements, it is not a catchall solution (Parent, 2005). However, it is generally accepted that the positives outweigh the negatives.

A particularly hot topic of late in terms of E-Government is the use of social media or Web 2.0 technologies to support both singular and two-way communication. A 2008 study found that despite the lessons learned from Hurricane Katrina and the increasing use of social media by emergency management organizations an overall lack of understanding by leadership still existed as to the significant role that social media plays in communications (Guth, 2008). Since 2009, at least three theses on Web 2.0 and its use in government were written at the Naval Postgraduate School alone. These theses argue that social media provides an avenue for increased speed and efficiency in communications (Polania, 2010), improved information sharing (Bennington, 2010), and an increased ability to inform the leadership's decision-making process (Van Leuven, 2009).

2. Internet Anonymity

The literature on E-Government has not specifically explored the issue of anonymity. Significant research has been conducted on the topics of anonymity, privacy, and the security of information on the Internet, beginning with well-known cryptography expert David Chaum's 1981 paper entitled "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms." Anonymity is often discussed as a founding principle of the Internet, an explicit right, and the cornerstone of Internet freedom (Diamond, 2010). Three distinct positions on Internet anonymity have been identified and defined by Ya-Ching Lee of the Institute of Communications Management at National Sun Yat-Sen University in Taiwan, as the Libertarian Model, the Private Enterprise Model, and the Statis Model. Simply put, the Libertarian model favors anonymity for individuals, the Private Enterprise model looks at limiting anonymity so companies can gather profiles on their customer base, and the Statis model reflects government's desire to limit anonymity due to security concerns (Lee, 2006). For the purposes of this review, the Private Enterprise model was not considered as the concerns of private industry are not critical in the security vs. transparency debate.

The pro-Libertarian model literature states that anonymity provides individuals freedom of expression and protection from government/corporate surveillance. Specifically, the Internet has provided an opportunity for people to fight back against oppressive regimes and experience freedom without the fear of retaliation (Diamond, 2010). Libertarians argue that the Internet is self-regulating, and applying Statis model regulations punish citizens and criminals equally (Akdeniz, 2002). Opponents of the

Libertarian model and supporters of the Statis model (not necessarily the same thing) argue that anonymity removes accountability, provides an opportunity for terrorists and criminals to act without consequence, and provides an open forum for racism and hatred (Davenport, 2002; Morrison, 2005). This conflict has equal support on both sides, and mirrors the issues associated with the balance of secrecy and transparency. David Sify, the founder of Technorati, illustrates the issue “Taking away anonymity would have a chilling effect on the Web. We’d lose important release valves like whistle-blowing… [although] accountability brings civility” (Barret, 2007).

While this debate remains primarily at a stalemate, a couple of authors propose pseudonymity as a middle ground. Instead of having an unlimited number of identities (associated with anonymity), they suggest having a limited number of alternate identities with which individuals can surf the web with possible, but limited, traceability associated with their pseudonyms (Zarsky, 2004). Ultimately, whether anonymity, pseudonymity, or strict identification is the answer, more research needs to be done. Specifically, for the purposes of E-Government, identifying how to validate information received through social media is another area, which lacks exploratory research and solutions.

3. Government Secrecy and Whistleblowers

A significant amount of literature discusses whistleblowers and their role in the government secrecy/transparency debate. The discussion has been reinvigorated by “cablegate,” the release of hundreds of thousands of classified Department of State cables to the website Wikileaks (Rosenweig, 2010). While the debate over the role of media and the Internet in whistleblowing activities is very active, widespread agreement exists among scholars and the government regarding the problem of over-classification and the role of whistleblowers in providing transparency in government affairs.

The U.S. Government has repeatedly and openly acknowledged the problem of over-classification. In a statement to the U.S. House of Representative’s Committee on Government Reform, Director of the Information Security Oversight Office J. William Leonard stated, “it is no secret that the [U.S.] Government classifies too much information (T. Devine, 2011)." At his confirmation hearing, Director of National Intelligence James R. Clapper stated, "We do over-classify. We can be a lot more liberal, I think, about declassifying, and we should be (Aftergood, 2010a)." Even President Barack Obama publicly acknowledged, "effective measures to address the problem of over-classification" (Aftergood, 2010a) are needed. Over-classification leads to a degradation in U.S. ability to engage in homeland security efforts effectively by reducing the flow of critical information across agencies and levels of government (National Commision On Terrorist Attacks Upon The United States, 2004).

Speculation has arisen as to the costs and consequences associated with over-classification; however, there have not been many definitive answers identified through studies. Some authors argue that excessive government secrecy and over-classification has reduced government accountability by obstructing the public's ability to seek disclosure of government-held information (The Constitution Project's Liberty and Security Committee, 2009). The Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission Report) found that existing trends of over-classification and secrecy deprived intelligence and law enforcement of a potent weapon against terrorism: an alert and well-informed American public (National Commision On Terrorist Attacks Upon The United States, 2004). In FY2009, alone, the costs associated with government security classification were approximately $8.8 billion dollars, not including intelligence agencies' expenditures (Kosar, 2010). More research needs to be done to demonstrate the real costs and benefits, both financial and social, of addressing the over-classification problem. Still, current policy and legal solutions to the over-classification problem are limited and unimaginative for providing for a significant role for whistleblowers to play.

Clay Shirky, an author and expert on Internet technologies and their social impact, writes,

> For many of our most important social systems, we resolve clashing principles by providing an escape valve, in the form of a set of actors who are less rule-bound than the rest of the system. The most famous and ancient is the jury, a collection of amateurs who can, in the face of clear

> laws and evidence, simply not return the verdict a judge would have returned. So with secrecy. Though I am not a lawyer, the Supreme Court's 1971 ruling seems to say that there is no law-like way to balance the State's need for secrets with the threats secrets pose to democracies. (Shirky, 2010)

In the context described above, Shirky is not alone in the idea of whistleblowers as the "non-law like way" to address secrecy; in fact, both the academic and government communities support the actions of whistleblowers as necessary to report fraud, waste and abuse in government (Verschoor, 2010; Vandekerckhove, 2010; Smith, 2010; Fisher, 2005). Congress has gone as far to say, "All Federal employees are ethically bound to expose violations of law, corruption, waste, and substantial danger to public health or safety" (Committee on Government Reform, House of Representatives, 2006).

In addition to the widespread agreement of the importance of whistleblowers, general acknowledgement also exists that whistleblowers face significant risks of retaliation and reprisal (Goodman, 2007; Project on Government Oversight, 2005; S. Devine, 2010), and that current whistleblower protections are inadequate (U.S. Office of Special Counsel, 2004; Mihm, 2001; U.S. Merit Systems Protection Board, 2010; Committee on Government Reform, House of Representatives, 2006). Many authors have provided policy recommendations to address retaliation; however, most of the recommendations are focused on managing the consequences after retaliation occurs. Very little research discusses the possibility of addressing the problem from a prevention standpoint. Two current government efforts are happening to leverage technology and anonymity to promote whistleblower activities, the Government Accountability Office (GAO)'s FRAUDNET (Government Accountability Office, 2009) and the Department of Defense's 'Defense Hotline' (Department of Defense Inspector General, 2007). An opportunity exists to study the lessons learned from these two government programs, and examine the possibility of addressing the issues of whistleblower retaliation and reprisal through the application of some anonymity technologies.

The topics of E-Government, Internet anonymity, and whistleblowers have each individually been broadly covered by the current field of research. However, a detailed evaluation or discussion of the interrelationships between these concepts has not occurred. For example, how to verify the accuracy of the information being provided by the public, if the submission is anonymous? This thesis explores those relationships for the purposes of identifying realistic solutions in an attempt to answer what may be an unanswerable question—How to balance secrecy and transparency?

This debate has been ongoing at the center of American politics back to the days of this country's birth. As this republic was being established, the founding fathers were contemplating the questions regarding the role of secrecy in government affairs, and the extent to which political decisions and government actions should be transparent to the public. Much has changed over the last 200 years, and those changes have seen the U.S. Government's policies on secrecy and transparency shift between one end of the spectrum to the other. The shift is often the result of changes to the political, economic, and technological landscapes impacting this country, but a definitive answer to the underlying questions has yet to appear. How to decide what the public needs to know, and what to keep confidential? How to balance government accountability with national security interests? In the absence of agreement among government leaders and sufficient government mechanisms to ensure transparency to the public, traditional media organizations have long played a role as an external "watchdog" for government activities. The idea that traditional media organizations today are the same "free press" described by Jefferson is no longer accurate. The government's ability to influence and direct the media has increased substantially over the past few decades, and with economic trouble affecting traditional media organizations' ability to pursue investigative journalism, transparency has continued to decline, which is surprising considering the dramatic change in the information-sharing environment over the last decade. New technology, the rapid evolution of the Internet, and innovations in social media have provided the ability to gather and share information at an unprecedented level, and yet the amount of classified information in the government has continued to grow (Hall, 2005).

The government's failure to adapt to the new environment and adequately address the over-classification problem, as well as the traditional media's inability to serve as the government watchdog adequately, has created a public backlash. The recent disclosure of thousands of potentially classified documents by the website Wikileaks is an example of what is likely to be a growing trend. While the U.S. Government and much of the news media have immediately condemned the website, describing the disclosure as treasonous and calling for the termination of the site itself, a dissenting viewpoint does exist. Some argue that in the absence of sufficient and reasonable government efforts to provide transparency, and with a reduced ability of the news media to perform the 'watchdog' function, Wikileaks provides a service that bypasses the bureaucracy and provides vital information to the public. That instead of treason, Wikileaks is a 'whistleblower' website and it should be considered a positive tool in the pursuit of government transparency and accountability. Each of these positions represents the polar ends of the secrecy/transparency spectrum, extreme approaches that do not acknowledge the need for a balanced answer. To identify solutions that achieve that balance, it is critical to understand the principle elements at play, first and foremost: whistleblowing.

B. PERCEPTION OF WHISTLEBLOWING

Through a review of the considerable amount of research that has been focused on government whistleblowers, it is clear that the majority of employees who witness acts of wrongdoing choose not to report it. Despite the inaction of the overwhelming majority, there are those who do step forward and act, regardless of the potential consequences they face. What constitutes a whistleblower, what are the characteristics that set these individuals apart, and what psychological factors influence their decisions? This section will define whistleblowers, explore both the dispositional and situational factors that affect them, and ultimately, propose some key issues that must be addressed to support increased whistleblowing among homeland security employees.

Historically, significant support for whistleblowers has occurred within Congress and the public. Popular culture has seen the success of films, such as Serpico (1973), The Insider (1999), and The Whistleblower (2010), which honor whistleblowers as courageous champions of truth, standing alone in an environment of rampant corruption. Congress has also traditionally been pro-whistleblower, repeatedly passing and revising laws in an attempt to protect and even encourage whistleblowers to come forward. In her 2003 book, *Whistleblowing: When it Works- and Why*, Roberta Ann Johnson even goes as far to claim, "It is no surprise that regardless of party or ideology, Congress always passes whistleblower protective legislation unanimously" (Johnson, 2003). Unfortunately, that no longer holds true, definitely for Congress and possibly for the public at large. This change does not reflect increased support for corruption and wrongdoing, rather it stems from uncertainty surrounding the definition of whistleblowers and their actions. As stated previously, no generally accepted definition for whistleblowing exists; as such, it has come to mean different things to different people (Miethe, 1999). Significant cultural pressures have always existed not to break rank, with terms, such as 'snitch' and 'rat,' prominently used to describe people who speak out against their organization/group. Even among kids, 'tattle-tale' is used to label those who inform authority figures (teachers/parents) of misdeeds or wrongdoing. Current opponents of whistleblowers even go as far as using terms, such as 'traitors' to label them and their actions, seeking to invoke serious charges against them, including but not limited, to espionage and damaging national security. The environment created by these factors has allowed the definition of whistleblowing to be usurped and applied (by both extreme secrecy advocates and extreme transparency advocates) to people whose actions are not whistleblowing, but to those who, in fact, may have jeopardized national security. The release of hundreds of thousands of diplomatic cables and documents from both the Iraq and Afghanistan wars to 'Wikileaks' is an example of such a disclosure. The indiscriminant release of these documents, with no clear objective, to an organization that exercises the ability to shape the messages (alter the truth), is not whistleblowing. Debates have occurred as to the actual damage to national security caused by those releases; however, the presence of information that serves the 'public interest' is also unclear. Classifying this action as whistleblowing, which has been promoted by both sides of the transparency/secrecy debate, only serves to destabilize support for legitimate cases of whistleblowers, both in Congress and in the eyes of the public. The impact of the

Wikileaks disclosures on the perception of whistleblowers in Congress is exemplified by its inability to pass the Whistleblower Protection Enhancement Act (WPEA), specifically the anonymous hold placed on the bill in 2010 (Devine, 2011).

Two ways exist to address the perception issue: redefining whistleblowing, or replacing the terms whistleblower and whistleblowing with alternatives that do not carry historical baggage/controversy. This thesis focuses on the former—redefining whistleblowing and clarifying the key components of the definition. Alternatives to the term whistleblower exist, including "lamp-lighter," which if propagated, could help to address the negative connotations associated with whistleblowing, and should be considered for future use.

> I have always preferred the term "lamp lighter" to whistleblower. We can holler and shout but it's the lamplight that shines on corruption, injustice, ineptitude and abuse of power. We reveal villains as they try to scurry into the woodwork in hiding. We're often told: 'don't make so much noise' but we can reply, 'you'll soon hear noise enough before long'.
>
> - Frank Serpico (Project on Government Oversight, 2002)

C. DEFINING WHISTLEBLOWING

While no single definition exists, a few definitions are commonly used to describe whistleblowing. Ralph Nader, in 1972, used one of the earliest definitions, and states, "whistleblowing is an act of a man or woman who, believing that the public interest overrides the interest of the organization he serves, blows the whistle that the organization is in corrupt, illegal, fraudulent, or harmful activity" (Whistleblowing CEE Project, n.d.). Marcia P. Miceli and Janet P. Near, in 1982, proposed the most commonly referenced definition out of the academic field of whistleblowing research, which states whistleblowing, is "the disclosure by organization members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action" (Miceli, Near, & Dworkin, 2008). Finally, the U.S. Government defines a whistleblower as someone who "discloses information he or she reasonably believes: a violation of any law, rule, or regulation;

gross mismanagement; a gross waste of funds; an abuse of authority; a substantial and specific danger to public health; and/or a substantial and specific danger to public safety" (U.S. Office of Special Councel, 2010). While these three definitions have similarities, they each possess a distinct and yet critical element required for a complete definition of whistleblowing.

The role of whistleblowing in government, specifically its legitimacy and process, are often debated in terms of the whistleblower's motivations, the content/significance of the whistleblower's claims, and to whom the report is made. Not every act involving the disclosure of information should be considered whistleblowing (Whistleblowing CEE Project, n.d.); a clear definition of whistleblowing is required to delineate whistleblowing from other activities. For example, informants "are often involved in some sort of unethical affairs, and use disclosure for clarifying their own role, or reducing their liability" (Whistleblowing CEE Project, n.d.). This definition of informant could be further expanded to include anyone whose motivation for disclosure is self-serving in nature (profit, notoriety, etc.). To distinguish whistleblowers from other categories of behavior (e.g., informants, issue selling, taking charge, and inactive observers (Miceli, Near, & Dworkin, 2008), any definition of whistleblowing should include the three distinct key elements from the definitions above: "reasonably believes," "public interest," and "effect action." It is important to highlight that it may not be possible to determine the true motivations of employees who expose wrongdoing. Similar to the philosophical debate on the existence of altruism, it is impossible to prove. In all likelihood, whistleblowers' intent probably includes a mix of selfish and selfless motivations (Johnson, 2003). However, by including the phrase "acting in the public interest," much needed emphasis on the selfless part of intent is provided. Further, to prevent a debate over the significance/size of wrongdoing, which may impact the protections afforded the employee filing the claim, the definition of whistleblowing should not include subjective terms, such as "gross," "substantial," or "specific." The extent of the wrongdoing can be determined after the submission is made, and the purpose of the definition should be to encourage employees to come forward. A more complete definition of whistleblowing might look like the following.

> The voluntary disclosure by any man or woman acting in the public interest who reasonably believes that a violation of any law, rule, or regulation; mismanagement; a waste of funds; an abuse of authority; a danger to public health; and/or a danger to public safety has occurred and reports that information to persons or organizations that may be able to effect action.

For the purposes of supporting the process presented in this thesis, it is important to expound on the "persons or organizations that may be able to effect action" section of the definition.

In the computer security world, two types of vulnerability disclosures exist, full disclosure and responsible disclosure. Full disclosure can be defined as the disclosure of system vulnerabilities to the public with the intent of using public exposure to prompt rapid modification/adaptation to secure the vulnerability. Responsible disclosure can be defined as the disclosure of system vulnerabilities to the responsible party for a predetermined amount of time, to allow for modification/adaptation to secure the vulnerability prior to full disclosure. For a responsible disclosure policy to be successful, the possibility of full disclosure must exist. Organizations are more likely to take prompt action to address security vulnerabilities if they risk being exploited or losing face to the public, which is also applicable to government organizations and private sector critical infrastructure organizations as well.

D. PSYCHOLOGICAL FACTORS

> Throughout history, it has been the inaction of those who could have acted; the indifference of those who should have known better; the silence of the voice of justice when it mattered most; that has made it possible for evil to triumph
>
> - Haile Selassie, former emperor of Ethiopia. (Zimbardo, 2007)

Utilizing the proposed definition to define whistleblowing, and excluding those who report misdeed primarily (or solely) for personal gain, what drives whistleblowers to act? Significant research has occurred into the dispositional characteristics of whistleblowers in an attempt to determine if particular types of people exist who are more likely to be whistleblowers than others. It is easy to draw some assumptions regarding this question, including the oft promoted “whistleblowers are principled individuals with strong moral convictions and ethical employees, which has been prominent in the academic community” (Miethe, 1999). Many dispositional factors could potentially affect whistleblowers, including educational level, age, work experience, gender, marital status, and religious beliefs. Based on these factors, additional assumptions have been made that suggest that whistleblowers are more likely to be men who are better educated, have strong belief systems (religious), are more likely than others to endorse universal standards, believe in making sacrifices for the greater good, feel that people have a responsibility to prevent harm to others, and think they are persons of worth (Miethe, 1999). Regarding age and work experience, a number of conflicting assumptions have been drawn, with no clear and logical conclusion identified. Despite these assumptions, research conducted by Miethe on the dispositional traits of whistleblowers, to include personality and socio-demographic factors, indicates the lack of a strong difference between whistleblowers and other employees (Miethe, 1999). This research supports the idea that no specific whistleblower personality really exists, and instead, whistleblowers are more likely to act based on situational factors.

In *The Lucifer Effect*, Dr. Philip Zimbardo explores the power of situational factors, largely in the context of his Stanford Prison Experiment. In his chapter on social dynamics, Zimbardo explores the factors that impact situational power, and the studies that have demonstrated it. Concluding his chapter, Zimbardo cites a meta-analysis of over 100 years of social psychological research, including 25,000 studies and 8 million people, which demonstrates the robust and reliable impact of social situational forces (Zimbardo, 2007). Many of these situational forces affect a person’s decision as to whether to come forward as a whistleblower, and understanding those forces provide a greater opportunity to create an environment more conducive to whistleblowing.

It is impossible to discuss whistleblowing without addressing consequences. The U.S. Merit Systems Protection Board (MSPB) identifies the effect whistleblowing will have on an individual’s job, career and future as one of the most significant reasons why people do not become whistleblowers (Johnson, 2003). Sissela Bok, an ethicist, argues that the consequences of whistleblowing must be carefully weighed prior to acting, as they can cause severe damage to programs, agencies, and the people involved (Johnson, 2003). In her 1981 essay, “Blowing the Whistle,” Bok proposes a whistleblower checklist designed to facilitate the evaluation of three primary issues by the whistleblower—dissent, loyalty, and accusation. While the checklist is a good start to the discussion, it is clearly presented in terms of potential consequences to the organization. It does not acknowledge or account for the significant risks faced by the whistleblowers themselves. In “Whistleblowing At Work,” Miethe posits that “about half of all whistleblowers are expected to experience severe retaliation by management for their disclosures” (Miethe, 1999). Based on the realities faced by whistleblowers, specifically, the likely consequences they face (retaliation by harassment, reassignment, poor performance reviews, loss of clearances, and/or loss of the job), a risk category should be added to Bok’s whistleblower checklist. The checklist proposed in *The Art of Anonymous Activism* focuses almost entirely on the whistleblower, and could serve to provide balance to Bok’s whistleblower checklist.

Whistleblowing is often debated in terms of loyalty, specifically, weighing loyalty to the organization against loyalty to the public interest/moral principles. The conflict between these two forces is often at the center of the internal debate of employees deciding whether or not to come forward. Bok describes this dichotomy as “loyalty to the agency and to colleagues comes to be pitted against loyalty to the public interest” (Johnson, 2003). In 1980, Congress passed a Code of Ethics for Government Service, which required persons in government service to “put loyalty to the highest moral principles above loyalty to persons, party, or government department” (U.S. Government, 1980). However, the reality is that this is not a black and white issue, with many factors weighing into the debate. The type and severity of misconduct observed, the frequency of the misconduct, and the relationship between the potential whistleblower and the violator all serve to influence the decision to come forward. For some, loyalties to groups trump loyalties to moral principles. Following his acceptance of the Nobel Prize, Albert Camus stated, “I believe in justice, but I will defend my mother before justice” (Cusak, 2011).

For others, the loyalty to principle and their commitment to preventing harm outweighed all of the other factors. C. Fred Alford calls this the whistleblower's "choiceless choice" (Uys, 2011).

Two primary types of situational influences affect whistleblowers, group influence and the influence of authority. Zimbardo discusses both in *The Lucifer Effect*, describing group influence as "often indirect, simply modeling the normative behavior the group wants us to imitate and practice," while authority influence is "more often direct and without subtlety" (Zimbardo, 2007). Both can be seen as having significant influence over whistleblowers, creating an environment, which has the potential to encourage whistleblowing, although more often than not serves to discourage whistleblowing. Zimbardo calls this the "institutionalized evil of inaction" (Zimbardo, 2007). Although indirect and often more subtle, group influence is significant and can cause people to do things they might not ordinarily do on their own (Zimbardo, 2007). Group influence plays off human nature and what C. S. Lewis calls "the terror of being left outside" (Zimbardo, 2007), combining external forces, such as peer pressure with the internal desire to be part of the "in group." In both Muzafer Sherif's initial studies on conformity, and Solomon Asch's follow up studies, the results demonstrated that more often than not, people will give up their independent positions and follow a group mentality, even when they know the group is wrong (Zimbardo, 2007). The desire to be part of the group and not 'rock the boat' overwhelmed their independence, as the psychological costs associated with autonomy were too great.

Stanley Milgram, who built upon the foundations of Asch's studies and shifted the focus to determine how far someone would go under orders, has explored the extent to which authority figures have influence over people. In his first experiment, Milgram demonstrated how 65% of people would follow orders completely, despite expert predictions of less than 1% compliance (Zimbardo, 2007). Over the course of a year, Milgram conducted 19 different experiments in which he varied social psychological factors and measured their influence over his subjects. His data demonstrate it is possible to create an environment through a careful application of certain situational factors in which almost anyone could be either totally obedient or resistant to authority pressures (Zimbardo, 2007). The obedience effect demonstrated through these results have been replicated by a number of subsequent studies, further demonstrating the power influence that authority figures possess over subordinates.

Group influence and authority influence are not only able to cause action, but they are also able to create an environment conducive to inaction, which can sometimes be even more damaging. Zimbardo describes this influence as the "Institutionalized Evil of Inaction," stating that "in situations where evil is being practiced…there are often observers of the ongoing activities or people who know what is going on and do not intervene to help or challenge the evil and thereby enable evil to persist by their inaction" (Zimbardo, 2007). Bystander apathy, as demonstrated by the Kitty Genovese Case, is an unfortunate example of this. In 1964, 38 people in Queens, New York watched and did nothing as Kitty Genovese was killed outside her apartment (Johnson, 2003). While more recent analysis of the case casts some doubt on how many people actually saw the murder taking place, no question exists that many people heard the screams and still did not act (Zimbardo, 2007). Two factors help explain the lack of action by the witnesses: the need for interpretation created by ambiguity, and the fact that if others appear unconcerned, the less likely any one person will react (Johnson, 2003). These factors are also prominent in the whistleblowing environment, where ambiguity and the pressure not to break rank often combine and influence people away from whistleblowing. A former government employee once stated, "being a Democrat or Republican is just a party affiliation. 'Don't Make Waves' is a religion" (Johnson, 2003).

> [W]e must learn that passively to accept an unjust system is to cooperate with that system, and thereby become a participant in its evil
>
> – Dr. Martin Luther King, Jr. (Zimbardo, 2007)

Just as situational forces can push both action and inaction, so too can they promote heroism, as well as evil. Commenting on the 'banality of heroism,' Zimbardo remarks that the perpetrators of evil and heroism alike are just common, ordinary people; and that while neither attribute is the result of unique dispositional tendencies, both conditions (evil/heroism) emerge in particular situations and at particular times when situational forces come together to influence individuals to action (or inaction) (Zimbardo, 2007). The research by Miethe into a "whistleblowing personality" confirms that Dr. Zimbardo's statement rings true for whistleblowing as well. Whistleblowing is celebrated in *The Lucifer Effect* as a subtype of 'social heroism,' specifically defined as "individuals who are aware of illegal or unethical activities in an organization who report the activity without expectation of reward" and risk "jeopardizing carefully groomed careers, professional ostracism, loss of social status, financial losses, loss of credibility, and physical reprisal" (Zimbardo, 2007).

Despite the current environment being dominated by overwhelming pressure to conform and organizational loyalty prioritized and reinforced by authority figures, steps can be taken to modify the environment to be more conducive to whistleblowing. Zimbardo, discussing the possibility of a 'Reverse-Milgram Altruism Effect,' provides a 10-step process to resist unwanted influences (Zimbardo, 2007). Many of the 10 steps he proposes are applicable to the whistleblowing environment and should be promoted vigorously by homeland security leadership, which includes promoting (and exhibiting) accountability and personal responsibility, critical thinking, individuality and vigilance. The fourth of Dr. Zimbardo's 10 steps is "I will assert my unique identity," and it emphasizes that "anonymity and secrecy conceal wrongdoing [and] undermine the human connection" (Zimbardo, 2007), which is one area of focus where Zimbardo's conclusions are contrary to that factor's role in the whistleblowing environment. Significant research has been conducted into how deindividuation and anonymity lead to increased aggression and destructiveness. "Deindividuation creates a unique psychological state in which behavior comes under the control of immediate situational demands and biological, hormonal urges. Action replaces thought" (Zimbardo, 2007), which has also been researched in the context of internet interactions, specifically dubbed the 'Online Disinhibition Effect' (Suler, 2004). This theory attributes six factors: dissociative anonymity, invisibility, asynchronicity, solipsistic introjections, dissociative imagination, and minimization of authority, which combine to facilitate people saying and doing things online that they would not ordinarily do in face-to-face discussions (Suler, 2004).

In his article on Online Disinhibtion, John Suler discusses two types of disinhibition, benign and toxic. Toxic disinhibition is consistent with Zimbardo’s assessment of deindividuation and anonymity contributing to “rude language, harsh criticisms, anger, hatred, and even threats” (Suler, 2004). However, the research on whistleblowing suggests that not only can anonymity promote ‘benign disinhibition’ (the act of showing unusual kindness or generosity to others) (Suler, 2004), but in situations in which group and/or authority pressure occurs to NOT stand out or ‘make waves,’ anonymity can actually promote breaking rank and whistleblowing (Miethe, 1999)—defined by Zimbardo as a heroic act. By affording the availability of increased anonymity in authorized whistleblower submission processes, it is likely that the amount of whistleblowing overall would increase.

E. THE IMPORTANCE OF WHISTLEBLOWING

Modern society, as a whole, accepts and understands that misdeeds and wrongdoing occur, and implements measures to identify and correct those actions. Through the establishment of Inspectors General (IG), GAO and Internal Affairs in the public sector, and both internal and external auditing bodies in the private sector, organizations conduct self-evaluations and submit to outside oversight. Whistleblowing is an important part of this process, as whistleblowers are in a unique position to observe misconduct in their organizations (Miethe, 1999). Multiple studies have been conducted on fraud detection, and not only have the results of these studies supported the role of whistleblowers in detecting fraud, they even go as far to identify whistleblowers as the “single most effective source of information in both detecting and rooting out corporate criminal activity” (Kohn, 2011). PricewaterhouseCoopers conducted a study in 2007 that identified that whistleblowers uncovered 43% of corporate fraud (National Whistleblowers Center, 2010), while auditors uncovered 19%, and law enforcement 3% (Kohn, 2011). A 2010 study by the Association of Certified Fraud Examiners on Global Fraud concluded, “tips were by far the most common detection method. In our study, catching nearly three times as many frauds as any other form of detection…not surprisingly, employees were the most common source of fraud tips” (Kohn, 2011).

Whistleblowing allows organizations to identify issues, which can result in both financial savings and reduction of the potential for negative publicity and public backlash. Both Department of Defense (DoD) and the GAO have established fraud ‘hot lines’ to promote whistleblowing and accountability in government affairs. In 1998, DoD estimated that submissions to their IG hotline resulted in an average of $15 million per year (Miethe, 1999). In 2011, the Justice Department recovered more than $3 billion under the False Claims Act (Gamble, 2011), including the case of a company called American Grocers. This company was buying expired food at discounted rates, changing the dates on the food, and selling the food to the government at a significant markup. This food was to be served to American troops fighting in Iraq. The owner of the company was sentenced to 24 months in prison, and the Department of Justice reached a $15 million settlement with the company (Department of Health and Human Services, 2011). Delma Pallares, a whistleblower, initiated the government’s investigation into American Grocers (Knight, 2010). Thus, whistleblowers play a critical role in the identification of fraud and wrongdoing. Of the $3 billion recovered in 2011 by the Department of Justice, $2.8 billion of that amount (93%) was investigated as a result of whistleblowers (Gamble, 2011). This situation exemplifies Zimbardo’s 10th step, appropriately entitled, “I can oppose unjust systems” (Zimbardo, 2007). This mentality, above all, needs to be supported in government. The idea that ‘one person can make a difference’ should be promoted and reinforced using both authority influence and group influence. The goal should be to change the homeland security culture to support speaking out, and developing processes, which reduce personal risk to employees. It is only through the modification of the situational factors affecting potential whistleblowers that the DHS will be able to inspire more whistleblowers and more heroes.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANALYSIS

A. CURRENT STATE OF THE ENVIRONMENT: AUTHORIZED PROCESSES AND PROTECTIONS FOR WHISTLEBLOWING

1. U.S. Whistleblowing Policies

Whistleblowing in the United States is a complicated and risky proposition, with no fewer than 15 federal laws and upwards of 44 state laws, which address the issue in some way. Over the past few years, in particular, public awareness of whistleblowing has increased significantly; however, many misconceptions exist regarding the process and protections provided to whistleblowers in the United States. As the extent of U.S. law and policy on the issue of whistleblowing prevents an all-inclusive, in-depth review, this analysis focuses on the primary legislation impacting federal homeland security employees.

As defined by 5 U.S.C. § 2302(b) (United States Code), it is a prohibited practice for the government to engage in reprisal for whistleblowing—generally, a person with personnel authority cannot take or fail to take a personnel action with respect to an employee or applicant because of a disclosure of information by the employee or applicant that he or she reasonably believes evidences a violation of a law, rule or regulation; gross mismanagement; gross waste of funds; an abuse of authority; or a substantial and specific danger to public health or safety. The prohibition does not apply, however, if the disclosure is barred by law or is specifically required by Executive Order (E.O.) to be kept secret in the interest of national defense or the conduct of foreign affairs, *except* when such a disclosure is made to the Special Counsel, the IG, or a comparable agency official (U.S. Office of Special Counsel, n.d.).

The underlying basis for whistleblower protection is often identified as a constitutional right, having been established within the Bill of Rights, specifically, the 1st Amendment. Whistleblowing could certainly be considered a principle in practice with regard to freedom of speech. However, severe restrictions are placed upon federal employees that significantly limit their ability to disclose information in the first place (e.g., government secrets/classified information), mandating that they use internal administrative processes instead of legal action.

Significant case law serves to complicate the matter further. *Garcetti v. Ceballos*[1] (2006) established that the protection under the 1st Amendment is limited when speech is part of "official duties" (U.S. Supreme Court, 2006); however, subsequent rulings in *Posey v Lake Pend*[2] (2008), *Marable v. Mark*[3] (2007), and *Thomas v. City of Blanchard*[4] (2008), have been conflicting. Furthermore, the Civil Rights Act provides further support to the protections established in the 1st Amendment. However, federal law upholds the right of the president to classify information and restrict its dissemination, severely impacting the protections provided to homeland security whistleblowers within the constitution, which is an important example of how outside factors (e.g., legal rulings, agency actions, etc.) can have a significant impact on the interpretation and implementation of whistleblowing law.

Outside of constitutional rights, the primary law, which governs federal whistleblowers, is the Civil Service Reform Act (CSRA) and the subsequent WPA. The CSRA was established in 1978 and is generally acknowledged as one of the weaker whistleblower laws (Kohn, 2011), and, as such, it has seen multiple amendments. The

[1] In this 2006 case of a district attorney (Ceballos) who claimed he was retaliated against for criticizing the legitimacy of a warrant, the court ruled (in a 5–4 decision) that because his statements were made as a public-employee and not as a citizen, he retained no 1st Amendment protection (Duke Law).

[2] This 2008 case heard by the 9th Circuit Court of Appeals, dealt with a 'security specialist' employed by a school district (Posey) who expressed concerns to the school district regarding school safety and inadequate emergency plans. Posey suffered retaliation, and the district court ruled that his actions did not receive 1st Amendment protections per the *Garcetti* case. In this case, the appeals court overturned the district court's decision (The Recorder, 2008).

[3] In 2007, Ken Marable, a Washington State Ferry engineer, appealed a prior District Court ruling that his speaking out against corruption was not protected under the 1st Amendment. As in the *Posey* case, the 9th Circuit Court of Appeals overturned the District Court's decision (United States Court of Appeals, Ninth Circuit, 2007).

[4] In this 2008 case heard by the 10th Circuit Court of Appeals, the court overturned a District Court ruling that Ira Thomas (a building code inspector for the City of Blanchard Oklahoma) was not protected under the 1st Amendment for reporting suspected illegality per *Garcetti* (United States Court of Appeals, Tenth Circuit, 2008).

CSRA established the Office of Special Counsel (OSC) to protect whistleblowers from retaliation, while the Merit Systems Protection Board (MSPB) was authorized to hear and adjudicate reprisal complaints from whistleblowers (Lewis, 2010). Under this process, any appeals to the ruling of the MSPB are taken to the Federal Circuit Court. Unfortunately, under CSRA, up to 90% of whistleblowers lost appeals within the OSC/MSPB process, resulting in a significant decrease of whistleblowing over time (Lewis, 2010). To address this problem, Congress passed the Whistleblower Protection Act in 1989, which took steps to strengthen the OSC as an independent body; allowed for whistleblowers to take individual action if the OSC chose not to take their case to the MSPB, and eased the burden of proof on the employee to demonstrate that adverse treatment was due to whistleblowing (Miethe, 1999). Despite the attempts by Congress to address loopholes and shortcomings in the CSRA/WPA, major shortfalls continue to hamper legislation because of the interpretation of the laws by the courts and the implementation of laws by responsible agencies (OSC, MSPB, etc.). The Senate Committee report on the WPA even went so far as to state, "The Committee intends that disclosures be encouraged. The OSC [Office of Special Counsel], the [Merit Systems Protection] Board, and the courts should not erect barriers to disclosures which will limit the necessary flow of information from employees who have knowledge of government wrongdoing. For example, it is inappropriate for disclosures to be protected only if they are made for certain purposes or to certain employees or only if the employee is the first to raise the issue" (U.S. Senate, 2002). Despite what would appear to be clear guidance in support of whistleblowers, currently policies do not provide protections to employees who report wrongdoing in their chain of command, tell co-workers or those suspected of wrongdoing, challenge policies, are dictated, by virtue of their job description to find or point out wrongdoing; or are not the first to raise the problem. The impact of these loopholes is demonstrated by the fact that since 1999, approximately 94% of whistleblowers have lost appeals within the OSC/MSPB process, and whistleblowers have won only three cases out of 202 at the Federal Circuit Court of Appeals since October 1994 (Schwellenbach, n.d.).

It is important to note that while the CRSA/WPA provides protection, albeit limited, to federal employees, a “national security” exemption does exist. As defined by the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002, any employee who works for “the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, and, as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities (United States Code)” is exempted, and therefore, not covered by the WPA. While the DHS is not specifically identified in the legislation, instances occur when the Transportation Security Administration (a component of DHS) is specified as not being covered in the WPA, and clearly other components of DHS fall within the realm of ‘intelligence collection.’ Section 463 of the Homeland Security Act of 2002 states that pursuant to the exemptions identified above, “nothing in this charter shall be construed as exempting the Department from requirements applicable with respect to executive agencies—(1) to provide equal employment protection for employees of the department (United States Code).” This situation appears to be circular logic, stating that homeland security is not exempt from these protections, except when it is exempt from these protections. In an attempt to address the issues associated with exempt agencies, Congress established the Intelligence Community Whistleblower Protection Act of 1998, which served to reinforce its right to receive classified information from whistleblowers in the intelligence IC and allows for the Office of the IG to investigate whistleblower retaliation. Unfortunately, the ICWPA does not provide any protections to whistleblowers; rather it is only focused on procedures. The Federal Bureau of Investigation (FBI) has its own whistleblower protection statute, which also identifies the process through which FBI whistleblowers can submit information and the organizations responsible for the investigation of whistleblower retaliation claims. As discussed above, despite the intent of Congress through legislation, the interpretation and implementation of policies falls to individual agencies that have consistently demonstrated a lack of support for whistleblowers. Senators Grassley and Leahy even sent a letter to FBI director Mueller identifying a “concern…that the latest investigation was a sign of the FBI’s apparent haste to launch an OPR probe every time an agent speaks publicly about problems within the FBI” (Grassley, 2004).

The aforementioned U.S. policies only account for a fraction of the total federal policies in place regarding whistleblowers. A number of laws exist that are designed to incentivize whistleblowing, particularly in cases in which the government is being overcharged or defrauded. Under the False Claims Act, whistleblowers can receive compensation, to include a percentage of the total money returned from the disclosure, as a reward. The Frank-Dodd Act and the amended Sarbanes-Oxley Act, provide provisions for whistleblowers to receive rewards for reporting fraud in the financial sector. While these do not necessarily apply to the homeland security employee, (with the exception of the False-Claims Act), Frank-Dodd and Sarbanes-Oxley demonstrate an acknowledgement by the government that whistleblowing is important and should not only be protected, but rewarded as well.

2. International Policies for Whistleblowing

Despite the intent of Congress to support whistleblowing through the establishment of legislation, the United States remains behind much of the international community in providing the necessary guidance, incentives, and protections required to promote authorized whistleblowing. Through a review of international policies on whistleblowing, it may be possible to identify best practices that would be beneficial for a U.S. solution. The following four countries serve as a representative sample of foreign whistleblower policies, and provide useful information on promising practices and lessons learned.

a. United Kingdom

Whistleblowers in the United Kingdom (UK) are covered primarily under a single law, the Public Information Disclosures Act (PIDA) that came into effect July 2, 1999. PIDA is defined within its preamble as “an Act to protect individuals who make certain disclosures of information in the public interest; to allow such individuals to bring action in respect of victimisation and for connected purposes" (Government of the United Kingdom, 1998). While some similarities occur with the WPA and U.S. whistleblowing policies, PIDA presents a number of interesting and distinctly different approaches to whistleblower protections. PIDA provides coverage to all workers across all sectors, including temporary agency staff and contractors, home workers, police officers and every professional in the National Health Service. No minimum qualifiers exist (such as age and time of employment), however, like the U.S. WPA, it does not cover intelligence services and the armed forces (Public Concern At Work, n.d.). If protected employees suffers retaliation or are victimized as a result of their act, they are eligible to bring a claim before an Employment Tribunal, which can award damages (currently uncapped) based on the loss suffered, including the potential for additional compensation for aggravated damages and injury to feelings (Public Concern At Work, n.d.). Victimization can include dismissal, or, "any detriment by any act, or any deliberate failure to act, by his employer done on the ground that the worker has made a protected disclosure" (Government of the United Kingdom, 1998). PIDA defines protected whistleblowing when 1) a criminal offense has been committed, is being committed or is likely to be committed, 2) a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject, 3) a miscarriage of justice has occurred, is occurring or is likely to occur, 4) the health or safety of any individual has been, is being or is likely to be endangered, 5) the environment has been, is being or is likely to be damaged, or 6) information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

Whistleblowing policies in the UK were developed in an attempt to find the balance between the protection and promotion of public interest disclosures and the importance of organizational secrecy in free enterprise. The primary concern remains that whistleblower protections could be used to cover industrial espionage (Lewis, 2010). To achieve a compromise, PIDA establishes a 'three-tiered' approach for whistleblowers to report information. The first tier addresses what is often defined as 'internal whistleblowing,' or reporting the observed or suspected wrongdoing within the agency, organization or company. Unlike the U.S. WPA, PIDA automatically provides protection to internal whistleblowers (as long as they meet the required criteria), and allows for internal reporting either within or outside of their hierarchy/chain of command. For a disclosure to be protected at the first tier, the criterion is that the whistleblower has "a reasonable belief the information tends to show that malpractice has occurred, is occurring or is likely to occur" (Lewis, 2010).

The second tier in the UK process allows for disclosures to regulatory authorities, including the Financial Services Authority, the Health and Safety Executive or the Care Quality Commission (Public Concern At Work, 2010). While this tier is traditionally defined as 'external whistleblowing' or reporting the observed or suspected wrongdoing outside of the agency, this second tier allows external whistleblowing to occur in the absence of going to the broader public or society at large. By establishing a 'proxy for society' (Lewis, 2010), whistleblowers are given an alternative avenue to report wrongdoing without truly exposing those concerns to the broader public, as is the case with traditional external whistleblowing. For a disclosure to be protected at the second tier, whistleblowers must meet the criteria prescribed for the first tier. Additionally, the whistleblower has to reasonably believe "that the information and any allegation in it are substantially true and is relevant to that regulator (the organization to which the disclosure is made)" (Public Concern At Work, n.d.).

Lastly, in certain circumstances in which a valid cause exists to do so or the previous two tiers have failed, wider public disclosures will be protected (including to the media), as long as the disclosures meet the criteria for the first and second tiers and "are reasonable in all circumstances and are not made for personal gain" (Public Concern At Work, n.d.). Additionally, the disclosures must fall within one of the following categories: "the whistleblower reasonably believed he would be victimized if he had raised the matter internally or with a prescribed regulator; there was no prescribed regulator and he reasonably believed the evidence was likely to be concealed or destroyed; the concern had already been raised with the employer or a prescribed regulator; or the concern was of an exceptionally serious nature" (Public Concern At Work, n.d.). Reasonable disclosures are further evaluated based on the following circumstances: “the identity of the person to whom it was made; the seriousness of the concern; whether the risk or danger remains; and whether the disclosure breached a duty of confidence which the employer owed a third party. Where the concern has been raised with the employer or a prescribed regulator, the tribunal will also consider the reasonableness of their response. Finally, if the concern has been raised with the employer, the tribunal will consider whether any whistleblowing procedure in the organization was or should have been used” (Public Concern At Work, n.d.).

By using this tiered approach, PIDA not only provides encouragement to whistleblowers through its protections, it also serves to hold organizations accountable for taking corrective actions to address wrongdoing and to protect the whistleblower. If the first tier (the organization itself) fails to act, the second tier serves as a watchdog to ensure the issues are handled appropriately. Should the second tier fail in its responsibilities to hold the first tier accountable, the third tier serves to provide the same pressure and accountability (Lewis, 2010). By providing protection to those who report internally and identifying consequences for retaliation, the PIDA encourages employers to establish a clear process for whistleblowers and avoid retaliatory practices.

b. Belgium

Whistleblowers in Belgium, also called “denunciators” (Council of Europe—Committe on Legal Affairs and Human Rights, 2008), are afforded some protections based on the May 7, 2004 Whistleblowers Decree. This decree states that any civil servants can raise issues of negligence, abuse or irregularities (Council of Europe—Committe on Legal Affairs and Human Rights, 2008) to their supervisors, or directly to the internal auditing component of the Flemish Administration if their supervisor is involved in the wrongdoing (Lewis, 2010). If the whistleblower experiences retaliation or no movement on the issue occurs within 30 days, the issue can be submitted to the Flemish Ombudsman. Once under the protection of the government/ombudsman, any disciplinary actions against the whistleblower are suspended, and protection lasts until two years after the end of the investigation. Belgium goes further to support transparency by requiring the Flemish Ombudsman to report annually on all whistleblowing cases received, the status of the investigation and the ultimate findings. From 2006–2008, all cases submitted to the Flemish Ombudsman received protection from retaliation (Lewis, 2010).

c. Romania

Whistleblower protection in Romania was established with Law No. 571 of December 14, 2004, "regarding the protection of personnel within public authorities, public institutions and other establishments, who report infringements" (Romanian Parliament, 2004). Romanian whistleblower protections have some similarities to the UK's PIDA, however, while the UK legislation is balanced between the needs of the public and the needs of institutions/organizations, Romanian law favors the needs of the public. The law was established to protect members of "public authorities and institutions, the central public administration, local public administration, the government apparatus, public institutions, national companies, and autonomous administrations of national and local interest…[who]expose or report law infringements within public authorities, public institutions and other establishments, perpetrated by persons in leading or operational positions within public authorities and institutions" (Romanian Parliament, 2004). Law 571 stresses eight overarching principles, including legality, public interest supremacy, responsibility, non-abusive sanctioning, good administration, good conduct, balance, and good faith. Each of these principles provides guidance for the conduct of whistleblowers, as well as for organizations, agencies and the government. Whistleblowers are required (under the principle of responsibility) to provide data or facts regarding the reported issue (Romanian Parliament, 2004), and can report to any of the following: their supervisor, the head of their agency/organization, disciplinary committees in the public sector, legal bodies, investigative organizations, parliament, mass-media, professional bodies, trade unions or employee associations, and non-governmental organizations (Romanian Parliament, 2004). An important distinction between PIDA and Romanian law 571 is that while reporting through each tier is done consecutively in the UK (with some exception), Romanian whistleblowers can report to any of the above organizations "alternatively or cumulatively" (Romanian Parliament,

2004) as long as they meet the established requirements. Romanian law also provides for the ability to keep the whistleblowers identity secret if the person accused is either their direct or indirect supervisor (Lewis, 2010). Uniquely, Romanian law allows for whistleblowers to demand a press and union representative be present at any disciplinary hearings (Lewis, 2010).

d. Australia

Currently, no single, comprehensive legislation in Australia provides for whistleblower protection. However, eight independent acts (laws) that range from 1993–2003 cover eight Australian territories, and the Public Service Act of 1999, which covers the Commonwealth. Interestingly, Australia has been the focal point for a significant whistleblowing study. The “Whistling While They Work” (WWTW) project is a three-year collaborative national research project into the management and protection of internal witnesses, including whistleblowers, in the Australian public sector (Griffith University, n.d.). As part of its study, the WWTW team identified a series of best practices from the nine total Australian acts, which included the following key points: whistleblower laws must provide multiple avenues for disclosure, clear processes for submission should be identified, the role of disclosures to media/parliament need to defined, and Australia should pursue completely new legislation as opposed to amending previous acts. The WWTW project also identified the need for sufficient buy-in and support from leadership to ensure legislation is enacted, and ultimately, enforced appropriately. Much like the United States, Australia has proposed many bills to address whistleblowing; however, none of them, including the most recent Public Interest Disclosures Bill of 2007, has passed (The Parliament of the Commenweath of Australia, 2007).

3. International Best Practices for Whistleblowing Policies

Based on a review of the current U.S. whistleblowing policies and the best practices evident in the international whistleblowing policies above, the United States could improve six areas in its current policies by adopting some international best practices.

- **Who is covered**? The United States should establish a clear whistleblowing policy for civil service employees of the U.S. DHS, its detailees and its contractors. This single policy should cover all DHS components, including those identified as part of the IC and the Transportation Security Administration. Romanian law is a prime example of a policy that covers all necessary parties, and the United States can benefit from leveraging the eight principles identified in Romanian law to help shape U.S. policy. Additionally, U.S. policy should specifically remove the requirement to be the first to report wrongdoing.
- **What types of misconduct for reporting are covered**? It is a tremendous challenge to write any policy that covers, in detail, all possibilities and issues that could potentially qualify as misconduct. While the current U.S. policy identifies a number of specific categories that qualify as protected disclosures, the United States should consider including the phrase "issues of public interest," as identified in the UK PIDA.
- **What types of reprisals for reporting are covered**? As with the question above, it is nearly impossible to identify all possible reprisals or methods of retaliation that could possibly be used punitively against whistleblowers. While the U.S. language currently is broad with the use of "personnel action," clear issues exist concerning the interpretation or adherence to that language, particularly in terms of security clearances. The UK's PIDA uses the word "victimization" to define reprisals in terms of their effect on the whistleblower as opposed to the employer. While including this language may not prevent the prohibited actions from being taken initially, it may steer the investigation and adjudication in favor of whistleblowers and the U.S./DHS should take action in support of that objective.
- **When should legal protection begin and should there be a statute of limitations for filling legal action**? U.S. policy currently puts the burden on the whistleblower with regard to filing deadlines and requirements, as well as limitations on when protections begin and end. The United States should learn from Belgium and establish protection from the time of the initial submission until two years after the investigation has been completed.

- **How should employees proceed with a formal complaint**? The current U.S. model for whistleblower submissions is broken. As far as international best practices for processes, the three-tiered approach identified by the UK's PIDA is by far the most effective at balancing the needs of the public with the needs for the organization/secrecy. U.S. policies do not currently follow a tiered process, and explicitly do not cover internal whistleblowing. The U.S./DHS should establish a multi-tiered approach using similar guidelines as identified by the UK's PIDA, and utilize a proxy similar to the Belgian ombudsman.
    - **Tier-One: Internal**. Internal reporting should include submissions within the originating agency/component (to include within the whistleblower's chain of command) to the department's Office of the IG or the OSC.
    - **Tier-Two: External—Proxy**. External reporting should include submissions to Congress, and the DHS should establish a third party to coordinate on behalf of the whistleblower, similar to the Flemish Ombudsman. This coordinator could function as the proxy for society. Both Congress and the third party could serve as oversight and function as external auditing organizations over tier-one organizations, working with them to ensure the wrongdoing is addressed and to prevent reprisals/retaliation.
    - **Tier-Three: External—Public**. In circumstances in which neither Congress nor the third party is able to facilitate action on behalf of the whistleblower, the whistleblower or the third party (after a clearly established period of time) would have the option of submitting the information to the public/media. The whistleblower would retain protection as long as the criteria for public disclosure were met (identified in the PIDA and above).
- **Is whistleblowing incentivized**? U.S. policies are currently leading the world regarding incentivizing whistleblowing, specifically, under the Frank-Dodd and Sarbanes-Oxley Acts. However, those policies apply to the financial sector and no functional equivalent exists for homeland security employees. The U.S./DHS should enhance the False Claims Act or establish an incentive program to provide similar rewards to homeland security whistleblowers as is provided to financial whistleblowers by the Frank-Dodd and Sarbanes-Oxley Acts.

Based on the realities of the current whistleblowing environment and the issues associated with the authorized processes, employees are being encouraged either to stay silent or to report wrongdoing through unauthorized channels. While some of these channels have been around for hundreds of years, others are only now emerging from the new information-sharing paradigm of the Internet and Web 2.0.

B. UNAUTHORIZED PROCESSES FOR WHISTLEBLOWING

1. Fourth Estate

Traditional media organizations have played a role in the disclosure of secret information for hundreds of years. Politicians in British Parliament leaked information to newspapers for political gain in the 18th century (A Web of English History, 2009). Parliamentary proceedings were off limits to newspapers prior to 1770, and leaking was used as a tactic to force a debate beyond a stalemate or to a re-decision, through the impact of public opinion, which was primarily employed by calculating advantage-seekers who used the public to influence internal power struggles (Rosen, 2010). It is important to note that this tactic was effective only because of Parliament’s efforts to keep its proceedings secret. By restricting public access to all information, politicians could leak small portions of it that would provide only one side of the debate, usually that which would favor the side of the party leaking the information. This role of the press in government affairs was termed the “Fourth Estate” by Edmund Burke, comparing the function of the news media to that of the three houses then in Parliament (Rosen, 2010). The news media has continued, since that time, to play a key role in the leaking of political information, and, up until recently, newspapers and other media outlets were effectively the only ones that could publish and distribute something to a worldwide audience (Reinventing the News Room, 2010). The Pentagon Papers and the Watergate scandal are two examples of 20th century leaks to the news media that significantly impacted U.S. politics. However, the freedom of the press to pursue investigative journalism and to promote transparency and accountability has decreased significantly. As a result of economic difficulties faced by media organizations, pressure to compete with the entertainment industry, requirements for news desks to be profitable, and the increasing ability of the U.S. Government to influence news organizations, media’s role as a U.S. Government watchdog has declined significantly (Lloyd, n.d.). In the *Kansas*

News Media, columnist Bob Weeks writes, “The cure for a dishonest politician is an investigative reporter willing to allocate the time to expose the truth. However, the decline of resources at newspapers around the nation has increased the vacuum in …coverage. As such, newspapers around the country are curbing reporters’ ability to spend the time or money to investigate a story in addition to the daily beat they write” (Weeks, 2010).

In a recent Gallup poll, only 34% of Americans believe that U.S. media organizations are doing a good job in fulfilling their role as a watchdog of the Obama Administration (Saad, 2010). With the decline of investigative journalism, media organizations are then forced to become reliant on outside information sources—whistleblowers to provide the information on which they can report. The likelihood that whistleblowers will choose to release information to an organization is dependent on two primary conditions, the ability to maintain anonymity, and the ability of that organization to publish the material to a wide audience. With traditional news media organizations being pressured by the U.S. Government to release the names of their sources, anonymity can no longer be guaranteed (Shenon, 2010; Egelko, 2006). Additionally, with the recent release of information indicating that the U.S. Government successfully delayed, for over a year, the publication of information by the *New York Times* on warrantless wiretapping, as well as the increasing prevalence of “pay walls” on news websites, the perception of a traditional news organization’s ability to communicate the information to a wide audience has declined significantly (Democracy Now, 2008; Rosen, 2010). Thus, the media landscape is changing, and traditional news organizations are no longer the only game in town. As Edmund Burke’s ‘Fourth Estate’ has seen its effectiveness dwindle, a new Fifth Estate has been established and it is growing stronger every day (Sam Adams Associates for Integrity in Intelligence, 2010).

2. Fifth Estate

In June of 2009, Clay Shirky gave a talk at the U.S. State Department on the transformation of the media landscape and the impact that the new ‘social media’ has on the ability to exchange information. Shirky discusses the redefinition of U.S.

understanding of the relationship between the media and the public, from a one-way 'producer/consumer' relationship to a new paradigm where anyone can be a producer (Shirky, 2009). Traditional news media is increasingly finding itself on the consuming end, identifying and reproducing information that they have received from this new media paradigm or the Fifth Estate. The Fifth Estate consists of those organizations that exist beyond the realm of government control and authority, organizations, such as Wikileaks.[5] Wikileaks has been characterized as the "world's first stateless news organization," simultaneously existing 'everywhere,' bound by no one country's laws or jurisdictions, and releasing information without regard for any one national interest (Reinventing the News Room, 2010; Twitter:Wikileaks, n.d.). Wikileaks was born of the Internet, and like the Internet, they have no physical address or location of which to speak. Wikileaks maintains servers in multiple countries, has over 300 Internet addresses registered, and relies heavily on the free press laws of countries like Sweden and Iceland to offer it legal protection from the inevitable 'legal and political attacks' from governments and private companies whose secrets have been exposed (Assange, 2009). The description of what Wikileaks is often depends on where the information is coming from, and whether that source supports or protests the actions that Wikileaks has taken. The debate as to whether Wikileaks is a "whistleblower" organization, or a "treasonous" organization, continues to be fought on the front pages of newspapers, across the Internet, and in the public sphere worldwide (Associated Press, 2010; Baker, 2010). While not the first and certainly not the only website to offer leaked information to the public (Cryptome), their innovative use of technology and leveraging the power of the Internet has catapulted them to the front of the debate regarding secrecy and transparency in the 21st century.

Wikileaks is an information clearinghouse, described on its website as a "not-for-profit media organization [whose] goal is to bring important news and information to the public" (Wikileaks: About Us, n.d.). It was founded in December of 2006 by a small

[5] Individuals with blogs also can be included in the definition of the Fifth Estate.

group of anti-secrecy activists with the goal of creating an “intelligence agency of the people” (Symington, 2009). While that ambitious goal has be hampered by the many controversies surrounding Wikileaks as an organization, over the past four years, they have succeeded in releasing over 1.2 million documents to the public, more than the rest of the world’s news media combined (Nystedt, 2009; Assange, 2009). They have accomplished this release through their use of information technology to maintain sources’ anonymity, using “a convoluted network of Internet service providers, computer servers, hard drives, encryption and private, ‘virtual tunnels’” (Boyd, 2010). While leaks in the past have been person to person (or person to organization), the Wikileaks approach allows an anonymous source to provide information to an anonymous organization, providing a never before seen level of confidence in maintaining that anonymity (Boyd, 2010). Jim Lewis, the head of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington states, “with the Pentagon Papers, you had one fellow, Daniel Ellsberg, smuggling paper out the building and giving it to a reporter. Today, in the Wikileaks example, you have some unknown number of people who are able to contribute to a website that thousands, or even millions of people, can look at, right now” (Boyd, 2010) that is a model with which traditional news organizations cannot compete, and as a result, they are being forced to redefine their role in a “Wikileaks world” (Baxter, 2010). It is important to note, however, that Wikileaks is constantly adapting its model to be more effective, and part of their evolution involves a larger role for traditional media organizations. In an environment increasingly reliant on data, Wikileaks has experienced difficulty in distinguishing and focusing the world’s attention on significant data. Wikileaks found that when they released all of the data, along with their own commentary, the focus was not on the information itself, but on the significance of Wikileaks as an organization. Mr. Assange elaborates, “It’s counterintuitive, you’d think the bigger and more important the document is, the more likely it will be reported on but that’s absolutely not true. It’s about supply and demand. Zero supply equals high demand, it has value. As soon as we release the material, the supply goes to infinity, so the perceived value goes to zero” (Nystedt, 2009). Subsequently, Wikileaks has established an unofficial partnership with traditional media organizations, providing an embargo period to increase the exclusivity of the information to a single or a few organizations. Wikileaks' ability to leverage the technological capabilities of the Internet and to adapt and evolve as circumstances require, demonstrates some of the potential impact that 'Fifth Estate' organizations could have on the role of traditional media organizations and the future of information dissemination as a whole. In fact, as a demonstration of the success of the Wikileaks model for anonymous submission, both Al-Jazeera and *The Wall Street Journal* developed their own online whistleblower submission process.

Wikileaks is not without its share of controversies, and both reasonable and speculative concerns have been identified regarding their operations. Immediately after the first release of information on their website, Wikileaks was attacked on its credibility (Symington, 2009). A few weeks later, John Young (the founder of cryptome.org—a similar anti-secrecy website) accused Wikileaks of being a front for the CIA (Symington, 2009). Three primary issues have confronted Wikileaks, and continue to be explored by the U.S. Government and news organizations: the actions of Wikileaks will damage "national security" (Montalbano, 2010), they were irresponsible for not doing a thorough review of the information they released (Aftergood, 2010b) resulting in the release of the names of Afghan informants, which placed their lives in danger (Reals, 2010), and that their secretive spokesperson Julian Assange has alternate agendas (Assange, 2010) (and his own series of controversies). Julian Assange is currently fighting extradition on allegations of sex crimes in Sweden, while Wikileaks faces trouble of its own (Addley, 2011).

Much speculation is focused on the future of Wikileaks, and whether it will be able to continue to function given the tremendous opposition moving against it and the personal issues confronting Julian Assange. Ben Laurie, a member of the Wikileaks Advisory Board stated, "Wikileaks depends on the enthusiasm of a small number of people, and particularly on Assange. If he met with a nasty accident, maybe Wikileaks would fizzle out" (Symington, 2009). This situation does indeed seem to be a likely possibility, particularly with the recent reporting of an internal dispute that has led to some prominent Wikileaks staff members leaving the organization (Blodget, 2010). While some might see this as a sign signaling the end of Wikileaks, it is a shortsighted viewpoint. The existence of Wikileaks as an organization is irrelevant now, and their most significant contribution is not the release of 1.2 million potentially classified documents. The most significant impact of Wikileaks is their successful demonstration and validation of the 'Wikileaks model.'

The recent split may or may not portend the end of Wikileaks as an organization; however, it does provide a glimpse into the future of whistleblowing. In an interview with Der Spiegel Online, Daniel Schmitt,[6] the second most senior member of Wikileaks next to Assange, talks about his intentions moving forward outside of Wikileaks. He says, "I will continue to do my part to ensure that the idea of a decentralized whistleblower platform stays afloat. I will work on that now. And that, incidentally, is in line with one of our original shared convictions -- in the end, there needs to be a thousand Wikileaks" (Domscheit-Berg, 2010). Ultimately, the destruction of Wikileaks through the efforts of governments and/or private organizations will not end the leaking and proliferation of secrets. Don Burke, the head of the Central Intelligence Agency's "Intellipedia" project, has said that in 15 years, there will be no more secrets (Spaulding, 2010). Wikileaks has demonstrated the ability to leak and propagate information to a worldwide audience, and while this might seem to bolster the justification for the current U.S. policies and culture of over-classification, overloading the government classification system actually weakens its ability to protect the truly important information (Stewart, 2010). An old saying from 1960s and 1970s supports this premise, that "when everything is secret—nothing is secret" (Agrell, 2002), and if the United States continues on its path to try and maintain the status quo with regard to secrecy rather than adapting, it will find itself unprepared and behind the curve when the "lights are turned up" (Spaulding, 2010).

[6] His real name is Daniel Domscheit-Berg.

3. Secrecy and Over-classification

The current U.S. policies governing the management of classified information are inadequate in the face of the over-classification problem facing the U.S. Government. Despite the repeated statements from the current administration promoting increased transparency, including the issuance of E.O. 13526 and the passing of the Reducing Over-Classification Act by Congress, over-classification remains a serious problem facing the homeland security enterprise and the U.S. Government as a whole.

Franklin D. Roosevelt signed the first E.O. on Classified Information on March 22, 1940; however, the debate on the balance between secrecy and transparency in U.S. Government affairs dates back to Thomas Jefferson and Alexander Hamilton. Nineteen E.O. on Classified Information have been signed since Roosevelt's first E.O. 8381, the most recent of which is E.O. 13526 by President Obama in December of 2009 (Kosar, 2010). Unfortunately, none of the E.O.s has been able to answer the question, how to balance government accountability and public need-to-know against national security interests?

Three components comprise the classification issue: initial classification, personnel/policy implementation, and oversight/declassification.

- **Initial Classification**. The current guidance on classification levels are based on long-standing definitions of the three primary markings: confidential, secret, and top secret. Each description is based on the same concept, that "the unauthorized disclosure of [information] which could be expected to cause damage to the national security that the original classification authority is able to identify or describe" (Office of the White House Press Secretary, 2009). Little specificity exists regarding the definitions of these key terms, and currently, the definitions used by each classifier differs in the implementation of this policy. National Security is loosely defined as "the national defense or foreign relations of the United States" (Kosar, 2009), and no clear definitions exist that constitute 'damage,' whether 'serious,' 'exceptionally grave' or otherwise.
- **Personnel and the implementation of classification policies, accountability, and consequences**. The current estimate for the total number of people holding security clearances is approximately 2.4 million

(Aftergood, 2009). Each person has a different perspective on classification, varying levels of training, and very little accountability in terms of over-classification.

- **Oversight, information sharing and declassification**. Currently included are the provisions regarding the duration of classification, internal review processes for classified information, cross agency and public information sharing. Public disputes regarding classified information (Freedom of Information Act), whistleblowers, both legitimate and illegal (often determined ex post facto), and ultimately, declassification through the National Archives and Records Administration. Presently, little oversight occurs of classification actions, FOIA is inconsistently implemented, and Congress recently killed the Whistleblower Enhancement Act.

While E.O. 13526 takes some steps towards increasing government transparency and information sharing while decreasing the problem of over-classification, it only represents a moderate shift in the traditional secrecy vs. transparency spectrum. It relies primarily on policy changes, and while it hints at creating cultural change ("need to know" vs. "need to share"), ultimately its success will be won or lost based on the personnel implementing it. For example, the review of fundamental classification guidance is a positive step; unfortunately, it is, in many cases, being reviewed by the same people who implemented the incorrect guidance in the first place.

According to Clay Shirky, the world is currently experiencing "the largest increase in expressive capability in human history" (Shirky, 2009). Not only has the Internet drastically improved the ability to share information, it has drastically improved the ability to create information. With tools, such as Twitter (Twitter: About Us, n.d.), Facebook (Facebook: About Us, n.d.), and Usahidi (Ushahidi: About Us, n.d.), people can send messages around the world in near real-time and provide firsthand accounts of actions and events taking place. Governments worldwide are rapidly discovering that their ability to control information is dwindling, and Wikileaks is but one symptom of a dynamic change in the world of information as the world knows it. For the U.S. Government to protect its secrets, it requires a dramatic change in policy and approach: an acknowledgement that embarrassing secrets and proof of wrongdoing does not equate to 'national security,' that current government methods, such as Offices of the IG, the GAO and the Whistleblower Protection Act, do not equal an effective means to maintain transparency, and an acknowledgement that the media environment has compensated, and is, as a whole, beyond government influence. It is unrealistic to think that everything can be declassified, and both sides of the debate acknowledge that legitimate topics (e.g., nuclear weapons design) should be kept out of the public domain.

E.O. 13526 is only in its first year of execution and it is premature to say whether these steps alone will be effective. However, technology has changed the paradigm in which the world communicates and U.S. Government policies on classification and information sharing require a significant update. In light of the fact that leaks will likely increase over the coming years and secrets will become harder to maintain, the U.S. Government should support and expand upon the goals of E.O. 13526 and reduce its overall classified footprint, with a view towards restoring public trust. Achieving both these goals will ultimately contribute to the safety and security of the homeland.

4. Public Trust

Despite the commonly accepted and promoted concept of the importance of public involvement in government affairs, and the efforts of agencies, such as the DHS to increase public engagement, public trust has declined significantly during the past decade. A 2005 Harris poll determined that among Americans, only 27% trust the government (Covey, 2006), and according to the PEW Research Center, with the exception of a significant dip in November of 2001, distrust and anger towards the government has been rising to 86% as of April of 2011 (Pew Research Center, 2011). With regard to whistleblowing and transparency, the actions of the Obama and Bush administrations have only served to increase public (and whistleblower) distrust. The FBI’s pursuit of whistleblowers prompted Senators Grassley and Leahy to send a letter to FBI director Mueller identifying a “concern…that the latest investigation was a sign of the FBI’s apparent haste to launch an OPR probe every time an agent speaks publicly about problems within the FBI” (Grassley, 2004). Significant concerns were raised with the appointment of Scott Bloch to the OSC, which, in a 2004 GAO report, indicated that the OSC only met its statutory timelines 26% of the time and that 95–97% of its whistleblower cases were backlogged (Project on Government Oversight, 2005).

Additionally, Bloch was placed under investigation for alleged retaliation against employees; discrimination based on sexual orientation, and on April 27, 2010, pleaded guilty to criminal contempt of Congress and is facing jail time (Hsu, 2011). Creating a circumstance on which the head of the organization responsible for investigating retaliation on behalf of whistleblowers, is in fact, conducting retaliatory practices himself, combined with the Obama Administration's unparalleled prosecution of whistleblowers (significantly more than any previous administration (Greenwald, 2010)), has damaged public perception and trust in the government process.

When it comes to whistleblowing, trust is one of the most important factors, which guides the activity. In a MSPB study, three of the top four reasons why whistleblowers did not come forward had to do with fear of retaliation (Project on Government Oversight, 2005). However, trust as it has been traditionally defined (Giddens, 1990),[7] does not really capture the significance of trust in this context. When it comes to the relationship between whistleblowers and the government, Rashid and Edmondson's definition of 'risky trust' is more applicable (Rashid, 2011).[8] It is important to acknowledge whistleblowers' careers, reputations, and livelihoods are often at stake. If whistleblowers do not trust the government to act with their best interest in mind, they will continue to either stay silent, or report wrongdoing through unauthorized channels that do not have the same high level of personal risk associated with it.

5. Trust and Third Parties

The use of a third party to overcome trust issues in otherwise dyadic relationships are already commonly used in the areas of E-commerce, mediation, secure communications and online transactions (Blaze, 1996; Franklin, 1997). In *Building Consumer Trust Online,* Hoffman, Novak and Peralta state, "in the near term, this [lack of trust] cannot be easily resolved, but we can address it by giving consumers the

[7] A person's confidence in the reliability of another person with respect to certain outcomes.

[8] Risky trust exists when the magnitude of risk is significantly objectively higher than in most work or life settings.

opportunity to be anonymous or pseudonymous when engaging in information exchanges and online transactions," and that the goal is to provide "traceable anonymity," which "gives Web providers no clues about consumers' identities but leaves this information in the hands of a third party" (Hoffman, 1999). Leveraging the use of third parties to promote government accountability is not a new concept, and can be seen in the use of semi-independent investigation organizations (IG, and GAO, the 'watchdog' role of media as the Fourth Estate, and in the whistleblowing arena through the UK's three-tiered policy for whistleblower submissions, which uses a 'proxy for society' as its second tier (Lewis, 2010).

Previous attempts have actually be made by the government to leverage technology and anonymity to promote whistleblower activities, specifically, with the GAO's FRAUDNET (Government Accountability Office, 2009) and the DoD's 'Defense Hotline' (Department of Defense Inspector General, 2007), which all seem to support the concept of "horizontal accountability" as described by Mark Bovens.

> Partly in reaction to a perceived lack of trust in government, there is an urge in many western democracies for more direct and explicit accountability relations between public agencies on the one hand and clients, citizens and civil society, including the media, on the other hand. The latter should become forums of political accountability, so the argument goes, and agencies or individual public managers should feel obliged to account for their performance to the public at large or to civil interest groups, charities, and associations of clients. This would be horizontal accountability in the true sense, as the complete hierarchical chain, including Parliament, is surpassed and the agency, the minister, or the public manager is directly accountable to the citizenry. (Bovens, 2005)

The identification of the appropriate entity to function as the third party in this matter is critical. It could be argued that the government currently uses third parties already with regard to whistleblowers (through the use of IGs, GAO, and the OSC), however, in addition to the issues discussed above, all these organizations share the same flaw in that they are government bodies, funded through government channels and whose leadership is often politically appointed (Project on Government Oversight, 2002).

Whether this actually creates conflicts of interest or just the perception of them, they currently do not have the ability to serve as a facilitating third party and increase trust amongst the public.

6. Realities of Anonymous Reporting

The solution proposed by this thesis relies on the concept of anonymity to increase the likelihood of reporting. The concept of anonymity in whistleblowing is not new, nor is the implementation of solutions based on anonymity novel in government. The development and promotion of 'hotlines' in government were established with the passage of the Inspectors General Act of 1978 (Johnson, 2003). Since that time, the number of hotlines has significantly increased, as has their use. In 1989, the DoD Hotline received 12,000 calls per year, increasing, to 14,000 in 1992, and by 1997, the DoD hotline received 8,220 calls in six months. In 1997, the DoD Inspector General claimed that, since its inception, the hotline had saved the government over $391 million (Johnson, 2003). The DoD Hotline and the Inspector General's FraudNET program have even expanded to allow for 'anonymous' submissions through the Internet. However, significant concerns have been raised regarding the effectiveness and protections provided by hotlines. According to a report released by the Government Accountability Project in 1997, hotlines have "an abysmal track record in terms of investigation of allegations, substantiation of charges, and corrective action" (Miethe, 1999). In *The Art of Anonymous Whistleblowing*, the authors recount the story of a Chief Petty Officer who used the DoD Hotline to submit an anonymous report. The next morning he was called into his security officer's conference room and told a call had been received informing him that someone had tried to contact the IG. The security officer directed the Chief Petty Officer to "find the caller and plug the leak" (Project on Government Oversight, 2002). Stories like this highlight the problems associated with hotline use, including the inherent conflicts of interest of hotlines, which fall under the same organization as the reporting employee. When an administrative contracting officer for the Defense Logistics Agency tried to blow the whistle on her agency, she turned to the DoD Hotline after a number of unsuccessful attempts to get her organization’s management to investigate. The DoD Hotline referred the case back to her management for investigation, who closed the case as “unsubstantiated” (Johnson, 2003).

Significant concerns regarding confidentiality and anonymity provided by hotlines have been raised. While hotlines often provide claims of anonymity, they offer little or no protections other than the assurances granted through their privacy policies. Potential whistleblowers often do not understand the risks associated with communicating with hotlines, either trusting hotlines to strip out personally identifiable information, or assuming protections by calling, emailing, or submitting complaints via the Internet (see section on technology evaluation). This concern is so significant, that *The Whistleblower’s Handbook* goes as far to say, “don’t blindly trust corporate-sponsored hotlines” (Kohn, 2011). The concerns regarding confidentiality and anonymity expand beyond corporate/government sponsored hotlines. Following the success of the Wikileaks model for anonymous submission, both Al-Jazeera and *The Wall Street Journal* developed their own online whistleblower submission process. Shortly after their implementation, internet security experts panned both organizations (including a Wikileaks volunteer) and the Electronic Frontier Foundation (EFF) for promoting “false promises of anonymity” (Fakhoury, 2011). The general consensus of whistleblowing advocates is that hotlines have the potential to be useful, but significant risks are associated with their use. The EFF concludes their analysis of *The Wall Street Journal* and Al-Jazeera’s submission sites by stating “these websites are misleading and…use of them by people who risk prosecution or retaliation for bringing sunshine to corruption, illegal behavior, or other topics worthy of whistleblowing, is risky at best and dangerous at worst” (Fakhoury, 2011).

Over the past decade, an increasing number of whistleblowers have come forward, and despite the risks associated with their disclosures, many of them began by reporting wrongdoing within the authorized process. In some of those cases, it was only after they were unsuccessful in affecting change that they chose to seek assistance through unauthorized processes (the Fourth or Fifth Estate). Both the cases of Thomas

Drake and the recent issues with the Bureau of Alcohol Tobacco and Firearms ‘Fast and Furious’ program began as internal disclosures that did not result in action. Thomas Drake was a National Security Agency (NSA) employee who raised questions about the efficiency and effectiveness of some post-9/11 NSA programs to his management. After being dismissed, he submitted a report to the DoD IG’s office on what he reasonably believed was organizational wrongdoing by the NSA (including its telecommunications collection program). His next step was to inform Congress of the issues, and only after he had exhausted his authorized options, did he then decide to disclose the wrongdoing to the *Baltimore Sun.* He was tried under the Espionage Act, much like Daniel Ellsberg of the *Pentagon Papers*; however, all charges against him were dropped in return for his guilty plea against the lesser misdemeanor charge of misusing the agency’s computer system. Drake lost his job and his pension and now works at an Apple store (Zetter, 2010).

ATF Agent John Dodson had questioned his supervisors over the ‘Operation Fast and Furious,’ an ATF program, which, in an attempt to shut down weapons trafficking networks, allowed Mexican drug cartels to purchase weapons from U.S. arms dealers. Dodson’s management quickly reassigned him to another job, while taking no action to stop or modify the program. Following the death of U.S. Border Patrol Agent Brian Terry (by weapons purchased through the ‘Fast and Furious’ program), Dodson submitted a complaint to the ATF Office of Chief Counsel and Ethics section of the Office of the IG. While little action on the part of ATF leadership was taken, he was contacted by Congress, which proceeded to conduct an in-depth investigation. Six other agents came forward to support Dodson’s report on the ATF program. Dodson and three other agents were transferred to other offices, one agent retired, and the other agents involved with this issue have requested investigations into agency retaliation (Lajeunesse, 2011).

These stories support the information identified above, and serve as examples of how current processes for authorized submissions fall short of providing adequate whistleblower protections and often do not result in the redress of organizational wrongdoing. In the absence of action in the authorized process, whistleblowers turn to unauthorized processes to achieve their goals. The over-classification problem inherent in government only serves to encourage whistleblowers to make disclosures, and the lack of public trust in the authorized system causes them to seek unauthorized methods for disclosure. However, unauthorized processes also fail to provide whistleblower protection, and can result in the exposure of truly sensitive information that should be restricted for reasons of national security.

C. TECHNOLOGY EVALUATION

1. Current Technologies/Background

To develop potential solutions, the vulnerabilities of current technologies available for anonymous submission must be identified. Three primary means exist for a whistleblower to submit information to the government: over the phone, through email, or through the use of a web browser. While the phone can provide some anonymity and information security through the use of pay-as-you-go/disposable cell phones, major concerns are associated with discovery through other means (e.g., the purchase of the phone in the first place, voice recognition, the location associated with the origination of the call, etc.). These factors, combined with the inherent transmission limitations associated with using a phone (only verbal submissions, no documents, etc.), make the use of phones a possibility, albeit an unlikely solution, to this problem.

The systems associated with electronic communications are divided up into two categories, high-latency systems and low-latency systems. High-latency systems can experience and tolerate high delays in the transmission of information, and are generally used in non-interactive or non-real-time applications, such as email. Low-latency systems generally do not experience and have low tolerance for delay in the transmission of information, and are intended for use in real-time applications, such as web browsing, instant messaging, and VOIP (Mayer, 2009).

a. High-Latency Systems

Solutions for high-latency systems are able to provide some of the best anonymity available. Using technologies known as anonymous remailers, it would be possible for a whistleblower to submit information over email to the U.S. Government with strong anonymity protections. Anonymous remailers essentially serve as a middleman, forwarding the contents of the email to the recipient without the recipient receiving knowledge on the original sender's identity. In their 2009 paper, "On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems," Matthew Edman and Bulent Yenner from Rensselaer Polytechnic Institute provide an excellent description of the process.

> Imagine Alice is a corporate whistleblower who wants to mail a letter to *The New York Times* revealing some misconduct, but still wants to remain anonymous for fear of losing her job. Similarly to how IP addresses can reveal who sent a particular packet, simply writing a letter and dropping it in the local post office box would leak information to the recipient about where the message originated because of the postal markings on the envelope. Instead, Alice places the envelope addressed to *The New York Times* inside another envelope addressed to a third party named Charlie. This outer envelope is then placed inside yet another envelope addressed to another person, Sam. Alice then places the multiply enveloped letter into her local post office box. When Sam receives the envelope, he opens it and finds another envelope addressed to Charlie. Recognizing the envelope is not addressed to him, Sam then drops it in his local post office box. Similarly, when Charlie receives and opens the envelope addressed to him, he finds another addressed to *The New York Times*, which he then also forwards. Since the envelope received at *The New York Times* came from Charlie's post office, it does not give away any information about Alice's location. The envelope received by Sam can be used to identify Alice, but Sam only knows the next hop in the path and not the letter's content or its intended destination. Only if all people in the letter's path collaborate can they identify Alice as the sender of the letter received by the newspaper.

Remailers also provide added security in that not only do they forward the information, often times it will be mixed with other messages, placed in batches, and forwarded as a means to guard against unwanted observers. Three primary types of anonymous remailers exist: Type I or cypherpunk remailers; Type II or Mixmaster remailers; and Type III or Mixminion remailers (Remailers). Of the three, Mixminion

(Mixminion: A Type III Anonymous Remailer, n.d.) is the most advanced remailer available and can be used free of charge, unfortunately, however, it requires a level of computer savvy that the average government employee may not possess.

The use of email provides one of the best solutions from an anonymity perspective, although, it leaves much to be desired in terms of reliability and information security. Anonymous remailers are vulnerable to numerous types of attacks, suffer from unreliability concerning delivery, have significant issues associated with recipient replies, and have the potential to compromise the security of the information being transmitted. Email exists as a potential solution for the submission of non-sensitive unclassified information; however, a more robust solution is required to include additional measures, which ensure information security and address the whistleblowers' need for feedback.

b. Low-Latency Systems

The processes associated with high-latency anonymity solutions can create delays of many hours and even days prior to the completion of the transmission, a solution, which does not work in the low-latency environment of the web. However, the overarching concept associated with low-latency anonymity solutions is very similar to the one described in the Alice and *The New York Times* example above. The submitter (Alice in that case) could, through the use of one of the following three types of anonymity solutions; hide their IP address and location from the recipient (*The New York Times*). The three categories of low-latency system solutions are as follows: Proxy Servers, Virtual Private Networks (VPNs) and Onion Routing.

(1) Proxy Servers. Proxy servers are essentially a forwarding service (Sam, from the previously cited example), who, unlike the remailers described above, do not manipulate the data in any way prior to forwarding. A proxy server would allow the sender to submit data through a third-party network in a manner in which only the fact that the information came from a third party is discernible to the recipient. Basic web-proxy services, such as Anonwatch (AnonWatch, n.d.), are weak on both anonymity and information security; however, the proxy concept has spawned two additional solutions in the form of VPNs and Onion Routing.

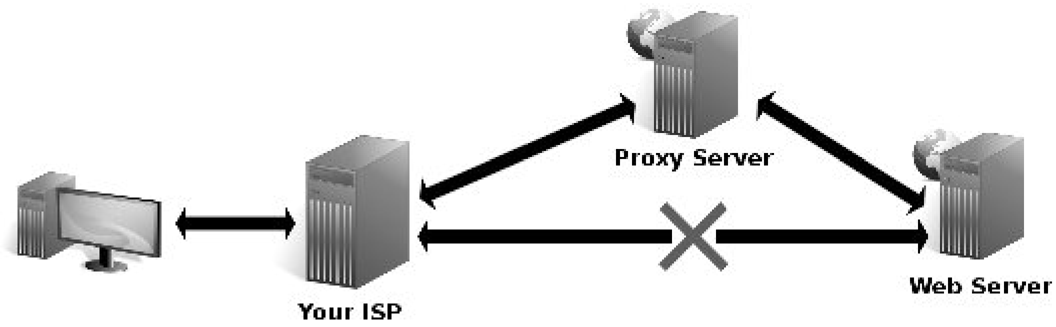


Figure 1. Information Flow Through a Proxy Server (From: Public Proxy Servers, n.d.)

(2) Virtual Private Networks. VPNs are currently used by the government and other organizations as the means through which an offsite employee can access its organizations' network resources by creating a secure tunnel between the organization's servers and the end user.

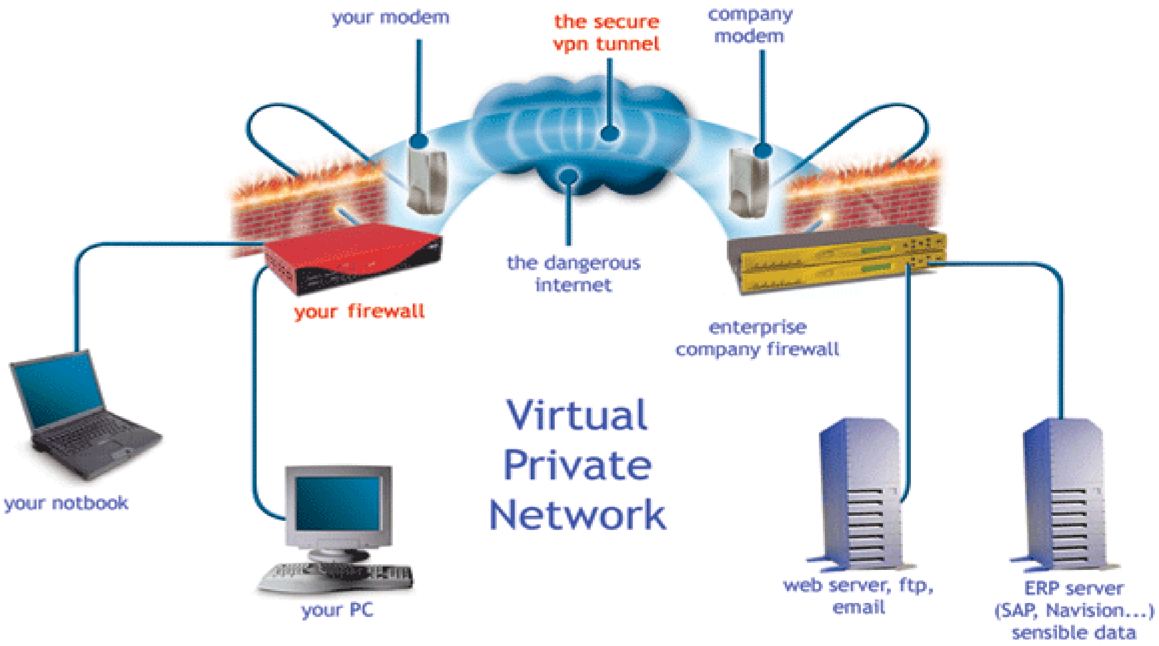


Figure 2. Using a Virtual Private Network (From: Hide Your IP Address with a VPN, 2011)

Relevant to the whistleblowing submission process, VPNs provide a paid for proxy server with end-to-end encryption, through which the sender would submit information to the government through the network provided by the third-party VPN provider, maintaining anonymity from the government. Significant issues are associated with the use of VPN technology for whistleblowing concerning both anonymity and information security. Regarding anonymity, while the use of VPN software allows the sender to hide his identity from the recipient, it does NOT hide his identity from the third-party VPN provider. The possibility exists that the government could subpoena or pressure the VPN provider to provide its logs, payment history, and/or other information that could compromise the identity of the sender.

VPNs also pose a potential problem in terms of information security; while a VPN does provide significant protection from the snooping of outside parties, the company itself would have potential access to the information being forwarded. The use of end-to-end encryption reduces this possibility significantly, but it is understandable that the government would be reluctant to provide a third-party company (many in foreign countries) access to sensitive information. Many pay-for-service VPNs are available currently, including StrongVPN (StrongVPN, n.d.), ViprVPN (GoldenFrog, n.d.), WiTopia (WiTopia, 20102), Anonymizer (Anonymizer, n.d.), and Xerobank (xerobank, 2012).

(3) Onion Routing. The approach used by onion routing is different from that of a VPN in that instead of one layer of anonymity protection (the VPN provider); multiple layers of anonymity protection exist (as described by Alice and *The New York Times* example above). The most prevalent onion routing system available, The Onion Router or TOR (Tor, n.d.a), was actually developed by the Navy (Onion Routing, n.d.) to provide anonymity and security in its communications. It was made public when it realized that if only the Navy was using the system, the anonymity set was 1, and therefore, it could not use it anonymously. Only when the user base of the system increased would the system achieve its goals. Instead of the single path identified by the VPN server, TOR selects random paths of three nodes from thousands of possible nodes, providing anonymity for the sender.

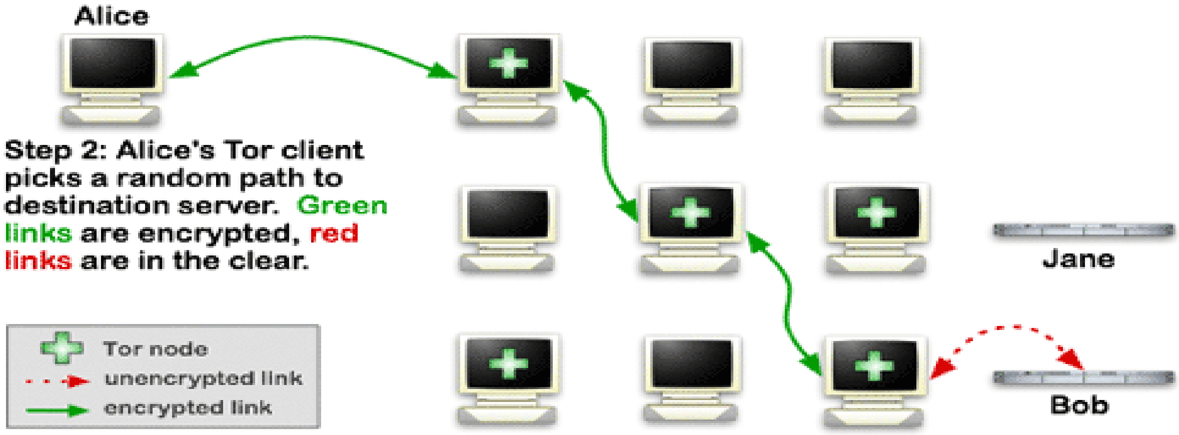

Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Bob
Tor node
unencrypted link
encrypted link

Figure 3. Accessing the Internet via TOR (From: Randomwire, 2011).

In terms of its potential for use in the whistleblowing process, TOR provides great anonymity for a single use submission, and with the use of end-to-end encryption (such as TLS/SSL), it also provides significant information security. Concern still exists from the government's perspective regarding sensitive information traveling through unknown nodes (even while encrypted). TOR is not the only solution available for the Onion Routing approach, Jondonym (JonDonym, (n.d.) and I2P (I2P, n.d.) are other paid solutions that claim to address some of the concerns associated with TOR's vulnerabilities and add some user-friendly applications.

c. *Vulnerabilities*

Many vulnerabilities are associated with the use of these technologies, including Traffic/Trend analysis (Hermann, 2009), Man-in-the-Middle (MITM) attacks (Zusman, 2009), Denial of Service (DOS) attacks, as well as identification vulnerabilities associated with cookies, JavaScript, flash, and other plug-ins that could bypass any system (VPN or Onion Router) and reveal the sender's identity (Clark, 2010). Concerns also exist regarding the use of public computers (for both anonymity and information security), the possibility of key loggers and malware compromising the senders' system, and the issues associated with anonymous payment for services (private VPNs, Jondonym, etc.). The research on vulnerabilities is extensive, with both the academic community and hacker community very active in pursuing both vulnerabilities and solutions. Over 40 publications exist on electronic anonymity, going back as far as 1981 on Freehaven.net, which provides in-depth detail on the issues identified above. However, for the whistleblowing environment, the researcher believes one or more technological solutions can be applied to provide protections through anonymity.

D. FINDINGS

The conclusions in this thesis could each be debated and explored in extraordinary detail as thesis topics in their own right. However, based on the research and analysis conducted above, the researcher has chosen to accept the following premises as true, and proceeds to focus on the solution to the defined problem.

- Overclassification is a problem
- Information sharing is critical to both U.S. security and U.S democracy
- Homeland security efforts require public (to include its employees and partners) trust and support to succeed
- The ability to keep secrets and maintain control of classified information will continue to decrease
- Decreasing overclassification will save the United States money
- Whistleblowing is a civic duty
- The government is committed to providing whistleblower protections
- Whistleblowers are in large part motivated by patriotism
- Anonymity is a positive incentive for whistleblowers
- Fourth and Fifth Estates provide alternatives to the government process
- Public trust in the government has declined
- Public trust can be increased through the use of third parties
- Technology exists to provide anonymity to whistleblowers
- Current options for whistleblowing are inadequate

These premises are important to understand prior to the identification and evaluation of potential solutions, as they form the foundation and justification for the implementation of any solution.

- **Over-classification is a problem**. The U.S. Government has repeatedly and openly acknowledged the problem of over-classification. In a statement by the Director of the Information Security Oversight Office, J. William Leonard, to the U.S. House of Representative's Committee on Government Reform, he plainly stated "it is no secret that the [US] Government classifies too much information" (Devine, 2011). At his confirmation hearing, the Director of National Intelligence, James R. Clapper stated, "We do over-classify. We can be a lot more liberal, I think, about declassifying, and we should be." Even President Barack Obama publicly acknowledged, "effective measures to address the problem of over-classification" (Aftergood, 2010a) are needed. What has not as yet been clearly defined and acknowledged is an understanding of the effects of over-classification, including its contribution to the unauthorized disclosure of information.

- **Information sharing is critical to both U.S. security and U.S. democracy**. Over-classification leads to a degradation in U.S. ability to engage effectively in homeland security efforts by reducing the flow of critical information across agencies and levels of government. Additionally, transparency through public information sharing is a critical component of U.S. democracy. Excessive government secrecy and over-classification has reduced government accountability by obstructing the public's ability to seek disclosure of government-held information (The Constitution Project's Liberty and Security Committee, 2009). An informed public is necessary to ensure that the U.S. Government is acting appropriately and in the best interests of the people for whom it purports to work.

- **Homeland security efforts require public trust and support to succeed**. The homeland security enterprise is comprised of entities from all disciplines and levels of government, including the public. From suspicious activity reporting and contributing to the deterrence of terrorist activities, to leveraging public preparedness to empower communities, help minimize fear, and diminish the effectiveness of terrorist tactics, the public plays a key role in homeland security efforts (U.S. Department of Homeland Security, 2010). *The Final Report of the National Commission on Terrorist Attacks Upon the United States* (9/11 Commission Report) found that existing trends of over-classification deprived intelligence and law enforcement of a potent weapon against terrorism: an alert and well-informed American public (National Commision On Terrorist Attacks Upon The United States, 2004). Over-classification and the accompanying lack of transparency may have eroded public trust in the government, resulting in a decrease in security as well. Additionally, decreased trust in government activities may result in additional leaks of classified information.

- **The ability to keep secrets and maintain control of classified information will continue to decrease**. Don Burke, the head of the Central Intelligence Agency's "Intellipedia" project, has said that in 15 years, there will be no more secrets (Spaulding, 2010). Wikileaks has demonstrated the ability to leak and propagate information to a worldwide audience, and while this might seem to bolster the justification for the current U.S. policies and culture of over-classification, overloading the government classification system actually weakens its ability to protect the truly important information (Stewart, 2010). An old saying from the 1960s and 1970s supports this premise, that "when everything is secret—nothing is secret" (Agrell, 2002). If the United States continues on its path to try and maintain the status quo with regard to secrecy instead of adapting, it will find itself unprepared and behind the curve when the "lights are turned up" (Spaulding, 2010).

- **Decreasing over-classification will save U.S. taxpayer money**. Particularly during the current time of economic concern, it is prudent to include the cost-savings associated with significantly decreasing U.S. Government over-classification. In FY2009, the costs associated with government security classification were approximately $8.8 billion dollars, not including intelligence agencies' expenditures (Kosar, 2010). By reducing the amount of classified information, the U.S. Government would see a decrease in expenditures associated with safeguarding information.

- **Whistleblowing is a civic duty.** Modern society as a whole accepts and understands that misdeeds and wrongdoing occur, and implements measures to identify and correct those actions. Through the establishment of IG, the GAO and Internal Affairs in the public sector, and both internal and external auditing bodies in the private sector, organizations conduct self-evaluations and submit to outside oversight. Whistleblowing is an important part of this process, as whistleblowers are in a unique position to observe misconduct in their organizations (Miethe, 1999). Multiple studies have been conducted on fraud detection, and not only have the results of these studies supported the role of whistleblowers in detecting fraud, they even go as far to identify whistleblowers as the "single most effective source of information in both detecting and rooting out corporate criminal activity" (Kohn, 2011). From the earliest days of this republic, as far back as 1778, Congress has repeatedly used the term "duty" to describe the act of whistleblowing.

- **The government is committed to providing whistleblower protections.** Whistleblowing is at the heart and soul of the 1st Amendment, establishing the right of the people to expose wrongdoing and demand accountability of their leadership (Kohn, 2011). Since that time, with the passage of the False Claims Act, the Civil Rights Act, the Civil Service

Reform Act and the subsequent Whistleblower Protection Act, Congress has displayed support for whistleblowers, using legislation to protect and promote the act of whistleblowing. It even has gone so far as to explicitly state, "The Committee intends that disclosures be encouraged. The OSC [Office of Special Counsel], the [Merit Systems Protection] Board, and the courts should not erect barriers to disclosures which will limit the necessary flow of information from employees who have knowledge of government wrongdoing" (U.S. Senate, 2002).

- **Whistleblowers are in large part motivated by patriotism and loyalty**. Research into whistleblowing has concluded that despite the assumptions to the contrary, no "whistleblowing personality" exists. The motivations for whistleblowers are neither total altruism, nor total self-interest. Whistleblowers are impacted more by situational factors than dispositional ones, and often are faced with a challenge of loyalties. Their "loyalty to the agency and colleagues often gets pitted against loyalty to the public interest" (Johnson, 2003), and they are forced to choose between the two, which has been called the "choiceless choice," for their loyalty to principle and a commitment to preventing harm in the service of the nation outweighs all other factors. Whistleblowers choose to act in the face of serious risks of retaliation and reprisal, and should be treated as performing a heroic act.

- **Anonymity is a positive thing for whistleblowers**. Overwhelming authority and group pressure to conform and prioritize organizational loyalty have dominated the current environment. Cultural and societal demands reinforce that pressure to not 'make waves' among employees. In these situations, providing employees with anonymity can actually promote breaking rank and whistleblowing, which can be seen in the increased use of hotlines and anonymous tips in government, law enforcement, and the private sector. Through increased availability of anonymity in whistleblower submission processes, it is likely that the amount of whistleblowing overall would increase significantly.

- **Fourth and Fifth Estates provide alternatives to the government process**. The Fourth Estate has played a role in government transparency back to the 18th century. The media has served as a government 'watchdog,' providing transparency and accountability through the application of public pressure. The Fourth Estate has provided whistleblowers an alternative way to achieve positive change, often without the personal risks associated with the authorized processes. However, with the decline of investigative journalism and the increase in political influence over the Fourth Estate, along with the rise of the Internet and social media as a communication platform, Fifth Estate organizations (such as Wikileaks) have provided whistleblowers another alternative. Through the application of anonymity via the Internet, and access to a worldwide audience, Fourth and Fifth Estate submissions provide greater incentives for whistleblowers than the current authorized processes.

- **Public trust in the government has declined**. As of April 2011, public distrust and anger towards the government had risen to 86 percent. With regard to whistleblowing and transparency, the actions of the Obama and Bush administrations have only served to increase public (and whistleblower) distrust. Creating a circumstance in which the head of the organization responsible for investigating retaliation on behalf of whistleblowers, is in fact, conducting retaliatory practices, combined with the Obama Administration's unparalleled prosecution of whistleblowers (significantly more than any previous administration (Greenwald, 2010) have significantly damaged public perception and trust in the government process. When further acknowledging that the Congressional approval rating has fallen to approximately 13% as of December 2010 (the lowest in Gallup history), little doubt remains that public trust has declined, and it will take significant efforts to rebuild it (Jones, 2010).

- **Public trust can be increased through the use of third parties**. Third parties have traditionally been used to overcome issues of trust, and examples can be found in the areas of E-commerce, mediation, secure communications, and online transactions. Even the government has used third parties to promote accountability through the creation of semi-independent investigation organizations, such as IG and the GAO. Guidance to whistleblowers often includes a recommendation to find an advocacy agent or proxy, who can serve to represent their interests and provide additional protections. Through the careful selection and application of a third party, the U.S. Government can increase its credibility and overall public trust in its efforts.

- **Technology exists to provide anonymity to whistleblowers**. While no technological solution can provide 100% anonymity, measures can be applied to provide significant identity protections for whistleblowers. Through the use of proxy servers, such as The Onion Router (TOR) or a third party Virtual Private Network (VPN), and 'good hygiene,' whistleblowers can significantly increase their ability to keep their identities secret (at least from the government organization to which they are submitting their report). However, anonymity often comes at the cost of information security.

- **Current options for whistleblowing are inadequate**. Currently, many options exist for both the authorized and unauthorized submission of whistleblower information. Authorized options come with significant risks to the whistleblowers, even in cases of government sponsored "anonymous hotlines," and the protections provided to employees via legislation are inadequate. Even fewer protections exist for employees of national security organizations. Based on the realities of the current whistleblowing environment and the government's inability to address these issues, employees are being encouraged either to stay silent or to report wrongdoing through unauthorized channels. However, unauthorized channels come with their share of drawbacks including issues with anonymity, the increasing ability of political pressures to affect Fourth Estate organizations, and the very real risk of the disclosure of information, which could have serious impacts on U.S. national security—particularly with Fifth Estate organizations.

IV. SOLUTIONS

> In national security there is a culture of confidentiality, the need to protect the nation's most sensitive information. In homeland security there's an expectation of transparency: it's not a need to know, it's a duty to share, it's an expectation to share. In national security there's unity of command. In homeland security, it's a unity of effort.
>
> - Jane Holl Lute, Deputy Secretary of Homeland Security (Bellavita, 2011)

A. DEFINITION OF SUCCESS

It is clear that whistleblowing serves as a checks and balances system for the government bureaucracy, helping to bypass administrative roadblocks and to provide a mechanism through which homeland security can monitor and increase efficiency in its operations. However, homeland security also deals with information that can be of a sensitive or secret nature, the unauthorized disclosure of which can cause damage to both homeland security efforts and national security. By creating an authorized process through which homeland security employees can submit whistleblowing information without fear of reprisals, it may increase the likelihood of whistleblowers reporting issues in the first place, and reduce the number of leaks to unauthorized recipients (media/stateless news organizations).

Based on the background and analysis sections of this thesis, specifically the conclusions above, it is possible to identify a number of potential solutions to the whistleblowing problem. However, prior to the evaluation of these solutions, criteria must be established by which any potential solution for whistleblowing can be measured. To develop evaluation criteria, it is important to define success for any whistleblowing solution. That definition is as follows:

> To promote the voluntary disclosure of information by any man or woman who reasonably believes that organizational wrongdoing has occurred, the facilitation of corrective action to address the wrongdoing, and providing for the protection of the submitter while maintaining information security, all within the bounds of U.S. law.

B. EVALUATION CRITERIA

Two primary objectives any whistleblowing solution must have to facilitate the whistleblowing process successfully are as follows.

- Acceptance by whistleblowers: In the absence of legitimate protections against retaliation, and based on the needs identified in the analysis, the recommended solution must meet or exceed the minimum needs of whistleblowers to be successful. The minimum needs for whistleblowers include the following.
    - Anonymity. Defined as the inability of the government sufficiently to identify the subject (whistleblower) from within a set of subjects (all government employees.) This definition has been derived from Andreas Pfitzmann and Marit Hansen's *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management—A Consolidated Proposal for Terminology.*
    - Feedback. Whistleblowers require feedback associated with their report, including confirmation from the government to the whistleblower that the information has been received and follow-up information regarding the action that will be taken.
    - Corrective Action. Whistleblowers submit their reports with the hope of facilitating corrective action to address the wrongdoing.
- Acceptance by the government: Based on the needs identified in the analysis model, the recommended solution must meet or exceed the minimum needs of the government to be successful. The minimum needs for the government are as follows.
    - Information Security. Defined as the protection of information from access, use, disclosure, disruption, modification, or destruction by unauthorized third parties. This definition has been derived from the U.S. Code, title 44 § 3542.
    - Legality and Political Acceptability. To implement any recommended solution, it must adhere to all current laws and legal requirements, and it must also be deemed "politically acceptable" or in 'government speak'—has to pass the "ho-ho test."
- Issues involving cost as an evaluative measure: Government activities are often measured using a cost metric, and based on (in situations where possible) return on investment. In this case, however, cost is not a primary evaluative factor, as it is extremely difficult to place value on homeland security whistleblowers (as opposed to corporate/wall street whistleblowing to the Securities and Exchange Commission that can be measured in a dollar value).

Using the above criteria, it is possible to evaluate potential solutions to the current problems facing government whistleblowers. While it would be difficult quantitatively to measure the criteria independently, a qualitative approach is useful whereby solutions are ranked relative to the status quo and each other for anonymity, feedback, corrective action, and for its ability to meet government requirements for information security. What follows employs theoretical sensitivity to conduct the "ho-ho test" (Tarbet, 2009) for political acceptability.

C. SOLUTIONS ANALYSIS

Current U.S. whistleblower policies attempt to provide protections by addressing retaliation and retribution after they have occurred, although success has been limited. As clearly identified in the analysis section of this thesis, the status quo regarding options for whistleblowers is unacceptable, with both authorized and unauthorized solutions failing to meet the evaluation criteria and falling short of achieving success as defined above. Through the innovative application of technology and the development or revision of the current DHS submission processes, it would be possible to provide whistleblower protections prior to retaliation.

Note: Solutions that involve direct disclosure to the Fourth or Fifth Estates has not been included. The legal status of Fourth Estate solutions (such as the sites set up by *The Wall Street Journal* and Al-Jazeera) is questionable at best, and falls short on the criteria for both whistleblowers and the government. Fifth Estate solutions are not permissible within U.S. law.

It is important to keep in mind that 100% security does not exist or is possible, just as regards 100% anonymity. The steps outlined herein are only one piece of the overall puzzle, and their success is very dependent upon the actions of both the submitter and the government. No process will work based on the needs of one party (government or whistleblower), and any solution will have to provide each with assurances and a level of trust in the process. If the government is committed to taking steps to prevent the unauthorized disclosure of information, it needs to provide an alternative that does not jeopardize the employee's livelihood.

At first glance, two possibilities may address both the whistleblowers and the Government's concerns.

These options are based on the following key components.

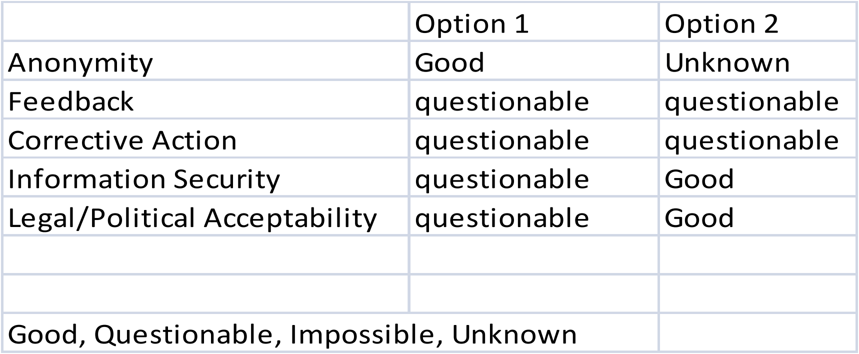
- The government establishes a submission site based on an apache-ssl server (or equivalent) to ensure appropriate end-to-end encryption is used to maintain information security.
- The government provides the 'public-key fingerprint' for its submission site to employees in a non-traceable way (perhaps in their "new employee packet" or on the DHS Intranet), to allow whistleblowers to authenticate the government's certificate and preventing Man-in-the-middle (MITM) attacks.
- Submitters practice 'good hygiene' with regard to their actions and submission, including stripping all identifiable information from their submission, running malware/spyware and virus scanners, and taking precautions when using technology to submit information (not browsing openly while they browse anonymously) to prevent overlap and java/cookie exploits.
- Submitters only use these options periodically. For example, if users are constantly submitting information to the government server using TOR, trend/traffic analysis can be used to identify them.

1. Option 1: Whistleblowers and Internet Anonymity

Option 1 is a solution almost entirely implemented by whistleblowers, using the Internet to provide anonymity as they submit to authorized government channels (such as the OSC, DHS IG, or GAO), which could be accomplished by using their home computer and by downloading and leveraging the TOR Browser (Tor, n.d.b.)—a self-contained instance of TOR with many of the vulnerabilities disabled. This option is primarily designed for the average government employee who does not have much experience with proxy/onion routing/VPN technology. Experienced employees could use Jondonym, I2P, or a third party VPN, as long as they are aware of the logging/information sharing policies of the company they choose. With this solution, it would not be possible legally to submit sensitive or classified information.

2. Option 2: Government Established VPN

In this case, the government would create a VPN service hosted by DHS or Congress. This VPN would be solely for submitting whistleblower claims, and access could be provided to all government employees. This VPN would provide anonymity to the submitter, while ensuring that any appropriate measures are taken to ensure information security. With this solution, it would be possible legally to submit sensitive or classified information.



	Option 1	Option 2
Anonymity	Good	Unknown
Feedback	questionable	questionable
Corrective Action	questionable	questionable
Information Security	questionable	Good
Legal/Political Acceptability	questionable	Good
Good, Questionable, Impossible, Unknown		

Table 1. Analysis of the Options

Anonymity: Option 1 is better than option 2 in terms of providing the best protections for the whistleblower, ensuring anonymity, which is largely due to the actual or perceived issues associated with government sponsored ‘hotlines.’ While the technology associated with option 2 may in fact be superior to option 1, public distrust in the implementation would likely result in few whistleblowers using the solution.

Feedback: Both option 1 and option 2 suffer from the same problem in terms of feedback. It is difficult for any solution to provide feedback while maintaining the anonymity of the submitter. Option 2 would have a slight advantage, in that the government could establish a process through which whistleblowers are issued a case number, and are able to follow up with their submission on a public site.

Corrective Action: As with feedback, both options fall short on this criterion. The likelihood of corrective action is not dependent upon how the submission is made, as any submissions to authorized recipients (IGs, GAO, or Congress) have the potential for inaction.

Information Security: Option 2 is clearly superior to option 1 in terms of information security. By using a government sponsored VPN, the information is more likely to remain securely within the government, while both TOR and third-party VPNs allow for the possibility of the information to be intercepted. Unlike with option 2, it would be impossible legally to submit classified information using option 1.

Legal/Political Acceptability: Option 2 is superior to option 1 in terms of legal/political acceptability as well. If the government chooses to institute a new policy for whistleblowers, it is more likely to be accepted and authorized than if whistleblowers took it upon themselves to use the Internet for submission.

In examining both options based on the evaluation criteria, it is clear that neither of these solutions has the ability to meet the needs of both whistleblowers and the government. Option 1 would likely be rejected by the government due to concerns about information security and legal/political acceptability, while option 2 would be disregarded by whistleblowers as not providing them protections through anonymity, largely due to lack of trust/credibility. Additionally, neither of these options has the ability to address corrective action in any way, making them unacceptable in terms of achieving success as defined above.

Nevertheless, with a review of the problem, the evaluation criteria, and the shortfalls associated with the first two options, a third possibility emerges. This option is based on the foundation for the technological solution proposed by option 2, but relies on a third party to address the issues of distrust and lack of credibility.

3. Option 3: Government Sponsored Third Party VPN

In this case, the government would form partnership with a NGO with credibility for promoting and maintaining anonymity, and authorize the creation of a VPN service hosted by the identified NGO. This VPN would be solely for submitting whistleblower claims, and access could be provided to all government employees. Policies would have to be established to ensure that the NGO would meet the whistleblowers' expectations of anonymity, while also ensuring the government's requirements for information security are met. With this solution, it would be possible to explore the submission of sensitive and classified information. Additionally, this option would also include a tiered reporting process, the application of which would prompt corrective action and provide accountability through escalation.

	Option 1	Option 2	Option 3
Anonymity	Good	Unknown	Good
Feedback	questionable	questionable	questionable
Corrective Action	questionable	questionable	Good
Information Security	questionable	Good	Good
Legal/Political Acceptability	questionable	Good	questionable
Good, questionable, impossible, unknown			

Table 2. Analysis of Option 3

Anonymity: Option 3 is superior to both options 1 and 2 in terms of providing the best protections for the whistleblower for anonymity. This option leverages the technological protections possible thorough the use of a third-party VPN (with strict policies against the logging of IP addresses), and with an appropriate selection of a third party, would lend credibility and increase public trust in the process.

Feedback: Option 3 suffers from the same problems as options 1 and 2 in terms of feedback. It is difficult for any solution to provide feedback while maintaining the anonymity of the submitter. Options 2 and 3 would have a slight advantage, in that the government could establish a process through which submitters are issued a case number, and are able to follow up with their submission on a public site.

Corrective Action: With option 3, comes the tiered reporting process, similar to the one discussed above, which would prompt corrective action and provide accountability through the possibility of escalation. In cases in which one tier fails to act, the next tier would be activated, which significantly benefit the government in that it would provide the opportunity to address reported issues prior to their public release (or instead of their public release).

Information Security: As option 3 is a government sponsored/approved third party and based on the technology solution proposed in option 2, it shares superiority to option 1 in terms of information security. By using a government sponsored third-party VPN, the information is more likely to remain securely within authorized government channels, while both TOR and unauthorized third-party VPNs allow for the possibility of the information to be intercepted. Option 3 is similar to option 2 in that it would be possible legally to submit classified information.

Legal/Political Acceptability: The one area in which option 3 falls short of option 2 is in terms of political acceptability. Legally, the government regularly authorizes third-party contractors to have access to sensitive and classified information. However, this option does push the boundaries of political acceptability both through the injection of a third party into the disclosure process and through the creation of a tiered submission process that includes the possibility of public disclosure.

The proposal of a third-party solution requires the development of additional evaluation criteria. Two primary factors drive the selection of the third-party organization, its ability to engender public trust and lend credibility to the process, and its current financial disposition. As with the application of any technology and the implementation of policy, associated funding must be available. To avoid conflict of interest situations, it is important that funding from the government be provided directly through Congress (instead of through one agency, e.g., DHS). The amount of funding the organization receives from the government (beyond just the funding for this process) should not exceed 2–3% of the organization's total income, and the organization itself must provide transparency on its budget numbers. Two additional factors should be noted, the organizations' willingness to participate in the process, and the government's willingness to engage with that organization.

Two types of non-governmental organizations could meet the criteria identified above. The first is whistleblowing advocate organizations, such as the Project on Government Oversight (POGO), the Government Accountability Project (GAP), and the Sunlight foundation. The second type includes Internet privacy and civil liberty organizations, such as the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC). A consortium approach could also be effective in the application of this process.

D. EDUCATIONAL CAMPAIGN

As discussed above, even if a technological solution was able to provide 100% confidentiality/anonymity (which it cannot), arguably the most significant vulnerabilities are associated with an individual's due diligence in scrubbing any information submitted for other potential identifiers. Electronic documents often contain watermarks and electronic signatures that can be tracked, emails can be used to identify the recipients, and the more limited the access associated with the information being submitted, the more likely the individual submitter could be identified. For example, the submission of details from a meeting with few attendees or a sensitive memo or email with limited recipients would make it easy to identify the individual filing the submission. Both *The*

Whistleblower's Handbook and *The Art of Anonymous Activism* promote 'good hygiene' and identify 'self-help tactics' that whistleblowers can use to protect themselves. These tactics include understanding whistleblower's rights and limitations, avoiding breaking the law, identifying and using an advocacy partner (outside organization to act on the whistleblower's behalf), documenting information thoroughly, and not using government resources or operating on government time (Kohn, 2011; Project on Government Oversight, 2002). This information would need to be made publicly available to any employee considering whistleblowing to ensure awareness of the risks, so that the appropriate measures can be taken to decrease the likelihood of identification and potential retaliation. Furthermore, the education of employees as to the process itself needs to be a high priority. In an American Federation of Government Employees (AFGE) survey, 87% of respondents were not aware of how to contact their whistleblowing hotline, 62% did not know where to get the number, and only 22% had seen the number posted in their work area (Johnson, 2003). By prioritizing and promoting responsible disclosure through the modification and utilization of existing trainings (such as the No Fear Act training), online information sites (DHS Intranet), employee welcome packets, reminder emails and posters (such as the Operational Security posters found everywhere in DHS offices), employees can be informed of the process for responsible disclosure, as well as the associated risks.

E. PROCESS FOR INVESTIGATING ANONYMOUS TIPS

Some concerns about the impact of anonymity on whistleblower submissions have been raised, as it decreases accountability for employees making accusations. It is important to bear in mind that although this process encourages whistleblowing by providing the protections associated with anonymity, not every submission will merit action or in-depth investigation. A vetting process associated with whistleblower submissions must exist, including a prioritization (by perceived significance) and a preliminary investigation (to determine merit). Prioritization can be assisted through an identification of significance by the whistleblower during the submission process. For example, national security vulnerabilities may be of high significance/priority, while human resource complaints and issues may rank lower. With the realities associated with limited resources for investigating agencies (IG, the OSC, etc.), prioritizing submissions prior to the conduct of preliminary investigations may help address the expected increase in whistleblower submissions.

The current OSC investigation process serves as an informative model on how to conduct investigations into whistleblower claims. The OSC process is initiated through the submission of a whistleblower report. The OSC has 15 days to review the information and determine whether further investigation is necessary. If the OSC finds substantial indication of wrongdoing, it informs the appropriate agency head of the matter. That agency head is required to conduct an investigation and, within 60 days, identify the following: a summary of the disclosure leading to the investigation, a description of how the investigation was conducted, a summary of all evidence found during the investigation, a list of any real or apparent violations, and a description of any action either taken or planned to be taken in response to the violation. Upon receipt of the report, the OSC reviews it and provides it to the whistleblower, who then has 15 days to submit any additional comments to the OSC. The OSC then transmits the agency report, any comments added by the whistleblower, and any additional comments from the OSC to the President, congressional leadership, and the congressional committee(s) holding jurisdiction over the agency. It is also made public on file at OSC headquarters (Project on Government Oversight, 2002). While the OSC process provides a good framework for an investigatory process, some drawbacks and issues do exist, which must be addressed in the proposed policy for it to be successful. These issues include the concerns about confidentiality of the whistleblower, the issues associated with having the accused agency conduct its own investigations, and ultimately, the public availability of the report.

Through the application of an appropriate process, concerns regarding the legitimacy of anonymous submissions can be addressed. In cases of retaliation/reprisal against whistleblowers, the single most prominent tactic employed by accused agencies is to attack the whistleblowers on their credibility (Miethe, 1999; Kohn, 2011). By creating a process that utilizes anonymity, whistleblowers are removed from the equation entirely, including the questions regarding their motivations (money, notoriety, etc.). It is impossible to collect rewards under the False Claim Act if the whistleblower is not identified. Through this process, on the focus is on the pursuit of the truth regarding the accusations of wrongdoing, rather than questioning the whistleblower.

F. RECOMMENDATION

The conclusions drawn in this thesis, including the policy model ultimately recommended, is based on the research and the findings identified above. Assuming these premises are true, and based on current understanding of the problem, the evaluation criteria, and the potential solutions available, it is recommended that the government establish a partnership with a non-government organization within U.S. legal jurisdiction (e.g., EFF, EPIC, POGO), and subsidize the establishment of a government sponsored whistleblower submission website and VPN. The third party would provide information on how whistleblowers could access their VPN to submit their information, as well as best practices to follow regarding information security and maintaining anonymity. The NGO would have to create a strict policy regarding the logging of IP addresses. The third party would also maintain and update the submission website with information regarding the status of submitted reports.

This organization is a neutral third party, and would serve as a mediator between the whistleblower and the government. Its functions as broker on behalf of the whistleblower, submitting information to the government and following up to ensure the information was evaluated and appropriate actions were determined. This organization also functions to balance the secrecy/transparency debate, weighing the public interest against issues of national security. In cases in which the government has decided not to act (in either first or second tier submissions), the third party would have the ability to review the information, and discuss the issues with both parties (should the whistleblower choose to step forward). Decisions to escalate to public disclosure require careful considerations, which however, may be considered necessary in certain situations. This process promotes corrective action by the government in addressing organizational wrongdoing through the accountability provided by the additional tiers of review. Inaction on the part of one organization will be questioned by the subsequent level of oversight.

Of the spectrum of options, ranging from achieving all of the government's primary concerns to meeting the needs of whistleblowers, this option falls slightly to the right of center. It is not as extreme as allowing submissions to an organization like Wikileaks (which the status quo is currently encouraging) or the use of self-generated anonymity by whistleblowers. However, it does acknowledge the need for change in the government's whistleblowing procedures. By bringing an NGO into the mix, the government takes huge steps in rebuilding public trust and legitimizing the role that whistleblowers play in government affairs. Regarding political acceptability and information security, a precedent exists for NGOs (consultants, etc.) to have access to and store classified information. By certifying the submission and storage process/procedures, the government can be sure that information security requirements are met. Whistleblowers are more likely to trust a NGO to maintain their anonymity (particularly those with a track record like the EFF's). Establishing this policy provides whistleblowers who truly believe in improving government operations through the submission of information on fraud/waste/abuse or other types of concerns, a legitimate way to achieve their goal without risking their career and future on the weak whistleblower protections currently in place. While it may not completely eliminate leaks to the media or organizations, such as Wikileaks, the researcher believes those leaks will decrease as more whistleblowers give the government an opportunity to act on their submission. Additionally, by granting the NGO oversight ability, the government provides the whistleblower with a 'fail safe' mechanism. If the government fails to act, the NGO has the ability to escalate the release of information to the media/public. However, in those situations, the government can be sure to establish reasonable limits on that release (e.g., no names of informants, nuclear weapon design, etc.). Lastly, while this option is higher in cost than some other possibilities, it does achieve the best outcome for all parties involved.

Regardless of the solution pursued by the government to address this problem, four key pillars create the foundation for success.

- **Whistleblowers must have the support of leadership—**This position affects all aspects of whistleblower protection, from the ability of Congress to pass appropriate legislation, to senior leaders at the DHS and the OSC who must enforce that legislation. If sufficient support from leadership does not exist, whistleblowers will remain unprotected. Problems with the lack of clarity around the definition of whistleblowers, as well as the perception issues that have resulted from the Wikileaks disclosures have seriously damaged leadership support of whistleblowers. Until leadership can be convinced that authorized whistleblowing is something that warrants support, no solutions will ever be effective.
- **Legislation and policies must be clear and straightforward—**Current U.S. legislation is a maze of contradictions, exemptions, and loopholes. For whistleblowers to feel protected, legislation must be developed in a way that allows government employees to understand it, and government agencies to abide by it. Many attempts have been made by the U.S. Government to revise current whistleblowing policy; however, the most recent attempt was stopped by an anonymous hold placed on the passage of the Whistle-blower Protection Enhancement Act in Congress, despite its bi-partisan support (Devine, 2011). The key to the implementation of any solution is support, both from leadership and the public.
- **Whistleblowing policies must enforce accountability—**The multi-tiered approach for whistleblower submission forces initial organizations and oversight agencies to act upon receipt of a whistleblower's disclosure. By establishing authorized alternatives for submission, it allows whistleblowers to retain protection for escalating disclosures, while encouraging agencies to act appropriately to avoid consequences.
- **Authorized channels must provide at least as much protection as unauthorized channels—**With the current perception that whistleblowers can submit information anonymously to unauthorized recipients, such as the media or third-party organizations (such as Wikileaks), it is paramount that any government whistleblowing policy provide protections that surpass (or are at least equivalent to) the perceived protections provided through Internet anonymity and Fourth or Fifth Estate submissions.

G. DRAFT POLICY

To demonstrate the possibilities associated with implementing this solution, the following draft policy is presented. This policy highlights the findings and conclusions in this thesis, while demonstrating the feasibility of the recommendations. For the purposes of the policy below, the details associated with the name and contact information for the third party are false.

U.S. Department of Homeland Security Responsible Disclosure Policy

Purpose: It is possible that during the conduct of their everyday jobs, employees may witness a variety of types of organizational wrongdoing. Employees are then faced with a dilemma; do they stay silent, or report the wrongdoing? If they decide to report it, how do they go about it and to whom should they go? Reporting organization misconduct or 'whistleblowing,' is the duty of every employee, however, if conducted incorrectly or through unauthorized channels, the disclosure of sensitive information can have damaging effects. This policy is designed to establish the process through which DHS employees may conduct whistleblowing in a safe, secure manner, without unintended consequences, which can jeopardize homeland security.

DHS has partnered with the "Neutral (and yet) Trusted Party" (NTP) organization for the purposes of developing and executing this Responsible Disclosure Process. NTP has been funded by Congress to develop the Responsible Disclosure Information System (RDIS), a website where whistleblowers can submit information anonymously and receive feedback and status updates on their submission.

Goals of Responsible Disclosure:

1) Ensure that instances of organizational wrongdoing are reported in a timely and efficient manner.
2) Minimize the risks of retaliation and reprisals against employee whistleblowers.
3) Provide the opportunity for the Department of Homeland Security to address issues internally, prior to, or in place of (in cases involving sensitive national security information), full (public) disclosure.
4) Promote prompt adjudication and resolution of organizational misconduct by the Department of Homeland Security through increased accountability provided by oversight and the possibility of escalation to full disclosure.

5) Increase public trust in government and minimize the amount of antagonism that often exists between parties due to the lack of consistent and explicit disclosure practices.

6) Reduce disclosures to unauthorized parties by providing a clear and effective process for the appropriate reporting and correction of organizational wrongdoing.

Definitions:

Whistleblowing: *the voluntary disclosure by any man or woman acting in the public interest who, reasonably believes that a violation of any law, rule, or regulation; mismanagement; a waste of funds; an abuse of authority; a danger to public health; and/or a danger to public safety has occurred and reports that information to persons or organizations that may be able to effect action.*

Organizational Wrongdoing/Misconduct: *the actions by an organization or individual that result in 'a violation of any law, rule, or regulation; mismanagement; a waste of funds; an abuse of authority; a danger to public health; and/or a danger to public safety.'*

Responsible Disclosure: *the disclosure of organizational wrongdoing to the responsible party for a predetermined amount of time, to allow for modification/adaptation to address the wrongdoing prior to or in place of full disclosure.*

Limited Disclosure: *the disclosure of organizational wrongdoing to as few (specifically authorized) parties as possible, to prompt additional investigatory or corrective action to address perceived organizational wrongdoing prior to full disclosure.*

Full Disclosure: *the disclosure of organizational wrongdoing to the public with the intent of using public exposure to pressure accused organizations to investigate and address the organizational wrongdoing.*

Major Roles in Disclosure:

Reporter: the individual who witnesses and discloses the organizational wrongdoing/misconduct. Also known as 'Whistleblowers' or 'Lamplighters.'

Coordinator: the individual or organization that serves as a neutral mediator and works with the reporter and the Investigator to facilitate the whistleblowing process and to ensure that responsible disclosure occurs prior to full disclosure. Coordinators may serve as proxies for reporters, helping to verify claims, resolve conflicts, and mediate between parties to resolve *the* issue in a satisfactory manner, with a minimum of potentially harmful consequences. NTP serves as the Coordinator for the U.S. Department of Homeland Security Responsible Disclosure process. Also known as 'Ombudsman' or 'Advocates.'

Investigator: the individual or organization who receives the report and is responsible for determining whether there is merit to the claim for examining the accused. Tier One investigators include the Department's Office of the Inspector General, DHS Component Offices of *Inspectors* General, or the Office of Special Counsel. Tier Two investigators include Congress, the Government Accountability Office and the White House.

Leadership: the individual or *organization* that is able to effect action to address and correct instances of verified organizational wrongdoing.

Accused: the individual or *organization* about which the initial disclosure was made.

Who is covered: This policy covers all *civil* service employees of the U.S. Department of Homeland Security, its detailees and its contractors. This includes all DHS components, including those that are identified as part of the Intelligence Community and the Transportation Security Administration.

Tiers of Responsible Disclosure:

This policy is based on a tiered process for responsible *disclosure*. The three tiers are:

a. Tier-One—Internal: Authorized Tier One reporting includes the submission of reports within the originating agency/component (to include within the Reporter's chain of command), to the Department's Office of the Inspector General, DHS Component Offices of Inspectors General, or the Office of Special Counsel.

b. Tier-Two—External Limited Disclosure: External reporting includes the submission of reports to Congress, the Government Accountability Office or the White House.

c. Tier-Three—External Full Disclosure: In circumstances where neither Tier One or Tier Two is able to facilitate corrective action, full disclosure can be made to the media/public. Full Disclosure can only be initiated by the Coordinator.

All reports submitted will be reviewed initially through the first tier, at which point the decision to escalate to additional tiers can be determined by the Reporter or Coordinator. However, in situations where Tier Two investigations have not resulted in action, the Reporter **cannot** escalate to Tier Three without the consent of the Coordinator. The Coordinator is a neutral third party, serving as a mediator between the Reporter and the Accused/Leadership. They also function to balance the secrecy/transparency debate, weighing the public interest against issues of national security. Decisions to escalate to the third tier require careful consideration, but they may very well be justified under certain circumstances. This process promotes action by Leadership in addressing organizational wrongdoing through the accountability provided by the additional tiers of review. In the Responsible Disclosure Process, inaction will be questioned by the subsequent tiers.

Phases of Responsible Disclosure

1) **Discovery**—One or more individuals discover or witness activities that they reasonably believe constitute organizational wrongdoing

2) **Reporting—**A Reporter submits a report to the coordinator, who then removes any of the Reporter's personally identifiable information from the submission. The coordinator then forwards the report to an appropriate investigator, including the identity of the accused and the details surrounding the suspected wrongdoing. The Investigator and/or Coordinator will provide confirmation to the Reporter that their submission was received through the DHS Responsible Disclosure Information Site (RDIS) and that the submission has been assigned a unique case number for the submission.

3) **Investigation—**The investigator prioritizes and conducts a two part analysis to determine the merits of the submission: within 15 days, a pre-investigation analysis is conducted to determine whether further investigation is required. If it is determined that more analysis is necessary, a detailed investigation is conducted within 30 days, in order to confirm or disprove the accusations of organizational wrongdoing by the reporter.

4) **Adjudication—**Upon completion of the investigation, the Investigator and/or the Coordinator updates the RDIS with the investigation status. The Investigator details conclusions from their investigation to the DHS Leadership for a 15-day review period. Upon receipt of the Investigator's report, DHS Leadership will take action (where required) to address any legitimate issues.

5) **Follow-up—**DHS Leadership will provide information on their decision to (or not to) act, to the Investigator and Coordinator. The Coordinator will then update the RDIS with the actions taken by Leadership to address the issues. The Reporter has 30 days from the conclusion of the investigation phase (90 days from initial submission) to review (using their case number through the RDIS) and take appropriate action as necessary. Appropriate Reporter actions include providing additional information, coming forward as an identified witness (losing the protections of anonymity), or escalating to additional tiers as appropriate. In situations where rewards are applicable (e.g. under the False Claim Act), the Reporter will have the opportunity to come forward and claim them within this phase. Only reports on issues of wrongdoing that do not have National Security restrictions will be publicly available.

6) **Escalation—**In cases where the Investigator was unable to confirm organizational wrongdoing and/or DHS Leadership has chosen not to take action, the Reporter can escalate the report to a Tier Two Investigator through the RDIS. Should the reporter decline to continue to be involved in the process, the Coordinator can serve as a proxy for the Reporter, and escalate on the Reporter's behalf. At that time, the Responsible Disclosure process starts again.

Note: In situations where Tier Two investigations have not resulted in action, the Reporter **cannot** escalate to Tier Three. All Tier Three escalations must be conducted by Coordinator.

Responsible Disclosure of Classified Information:

There may be circumstances that arise which require the disclosure of classified information in DHS Responsible Disclosure Process. While the publically accessible RDIS can only be used for the submission of unclassified information (including Controlled Unclassified Information), the Responsible Disclosure Process does allow for the submission of classified information.

To submit a report on organizational wrongdoing that involves classified information, the following steps are recommended:

1. Submit a report on the RDIS that provides an overview of the issue, and check the “classified submission” box. This will alert NTP that a classified submission is forthcoming. In the overview, do not include any classified information.

Please note: in order to maintain anonymity, this information MUST be submitted to the Coordinator. Any submissions sent directly to an Investigator will retain personally identifiable information.

2. For SECRET information, submit supporting documentation through the Homeland Secure Data Network (HSDN) or the Secure Internet Protocol Router Network (SIPRNET). Submissions can be made to the RDIS through its classified site at http://NTP.SGOV.GOV/RDIS, or via email to RDIS@NTP.SGOV.GOV.
3. For TOP SECRET information, submit supporting documentation through the Joint Worldwide Intelligence Communications System (JWICS). Submissions can be made through http://NTP.IC.GOV/RDIS or via email at RDIS@NTP.IC.GOV.

Submitting information via a government computer (as is required with classified information) provides the opportunity for the identity of Reporters to be discovered through computer logs and monitoring. For additional information or support regarding the submission of classified information, please see the help page of the RDIS or call NTP at 1-800-555-1000.

Protections provided through the DHS Responsible Disclosure Process:

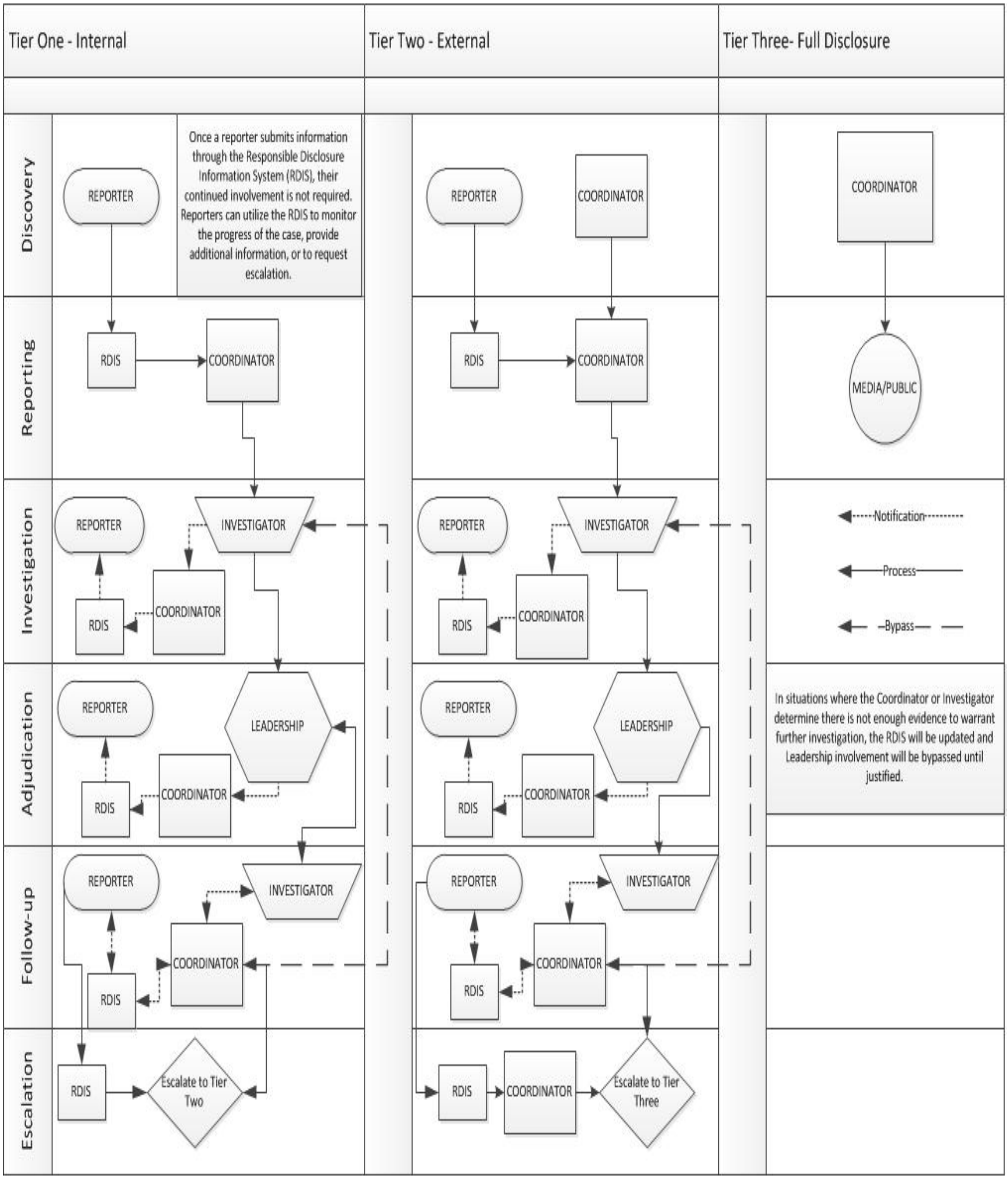
The NTP has created a Virtual Private Network (VPN), through which Reporters can securely submit information either to the Tier One Investigator of their choice, or directly to the Coordinator (NTP). In circumstances where the submission is to the Coordinator, steps will be taken to ensure any submission has been stripped of information, which could serve to identify the Reporter, prior to submission to an Investigator. NTP will then proceed to serve as a proxy for the Reporter, escalating through the tiers as necessary in the absence of Reporter participation.

This process provides Reporters (whistleblowers) with the protections afforded through the anonymous submission of reports. Additional protections can be provided by using the Coordinator to serve as a proxy for the Reporter (although that is not required in the Tier One or Tier Two). Reporters utilizing the Responsible Disclosure Process who suffer retaliations or reprisals for their actions are protected under current U.S. law, specifically the First Amendment and the Whistleblower Protection Act. In those situations, contact the Coordinator immediately to receive support and assistance. *Any Reporter who initiates the Responsible Disclosure process, who then proceeds to full disclosure* ***without*** *the consent/support of the Coordinator, forfeits all rights to protections and anonymity.*

RDIS is based on an apache-ssl server to ensure appropriate end-to end encryption is used to maintain information security. The public-key fingerprint for the submission site is available on the DHS Intranet, and can be used to authenticate the RDIS certificate and prevent ‘Man-in-the-middle’ attacks. In all cases, NTP will **not** log the IP address of the submitter. If possible, do not use DHS/Government computers to submit information to the RDIS (except in cases of classified disclosures), as this severely impacts the anonymity of the Report.

Reporters should practice good hygiene with regards to their actions and submission, including stripping all personally identifiable information from their submission, running malware/spyware and virus scanners, and taking precautions when using technology to submit information (not browsing openly while they browse anonymously) to prevent overlap and java/cookie exploits.

More information regarding the risks associated with Responsible Disclosure, and the steps Reporters can take to maximize their protections is available on the RDIS information page at www.whistleblowers.gov or www. responsibledisclosure.gov.



Once a reporter submits information through the Responsible Disclosure Information System (RDIS), their continued involvement is not required. Reporters can utilize the RDIS to monitor the progress of the case, provide additional information, or to request escalation.

In situations where the Coordinator or Investigator determine there is not enough evidence to warrant further investigation, the RDIS will be updated and Leadership involvement will be bypassed until justified.

Figure 4. Responsible Disclosure Process Flow Chart

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. IMPLEMENTATION ISSUES

The solutions proposed in this thesis have been designed in a way that allows for immediate implementation, utilizing currently available technology and carefully designed business processes (data rules) to provide protection to whistleblowers through anonymity. A limited scope pilot program, within one or more components of DHS, would provide an excellent opportunity to collect data on employee use of the process and to identify any issues prior to a large-scale investment of funds. While this thesis makes a convincing case of the importance of whistleblowers in government, a number of obstacles still stand in the way of implementation. For any realistic possibility of the implementation of this solution, it is important to have a clear understanding of the influential factors at play.

As a means of evaluating future utility of the solutions proposed herein, awareness of how the environment is likely to change in the near future must exist. Using a scenario based planning approach, three alternate futures capture (most of) the likely possibilities at a high level.

- Maintenance of the status quo
- Increased protection for whistleblowers
- Decreased protection for whistleblowers

By understanding each of these potential future states, it is possible to predict/evaluate the role (usefulness) that the proposed solution would have in each of the alternate futures. However, prior to the review of each scenario, some fundamentals are true regardless of the future environment.

The multi-disciplinary approach proposed by this thesis (the third-party partnership and business processes, combined with the innovative use of technology) is an example of disruptive innovation. The implementation of this solution would undermine currently established policies and processes for whistleblowers. Current legitimate/authorized processes, such as submission through standard government channels, present significant risks to the whistleblower. Clandestine/unauthorized processes, such as the Internet (Wikileaks) and mainstream media, represent a clear breach of the law, which is in conflict with the “do the right thing” mindset of many whistleblowers. If whistleblowers had a way to communicate identified issues through an authorized third party that would serve as a proxy on their behalf, it would undermine the current processes (both legitimate and clandestine), potentially making them obsolete. It would reduce the personal risk faced by whistleblowers by providing the anonymity that makes the clandestine approach attractive, without clearly breaking the law. If implemented correctly, the number of legitimate whistleblower complaints would increase (overall submissions would increase), and the number of whistleblowers who choose unauthorized avenues would be expected to decrease.

Regardless of which of the potential scenarios actually plays out in the future, some people/organizations will always remain that firmly reject increased whistleblower protections. The primary opponents of whistleblower protections (and solutions such as those presented by this thesis) will continue to be those politicians, government officials, government contractors and corporate interests that attempt to maximize profits and/or increase personal gains by skirting and/or breaking laws. Unfortunately, those people do not identify themselves by arguing that increased oversight of/transparency into their activities damages their ability to break the law. Instead, they have co-opted a legitimate concern regarding the need for government/corporate secrecy, and maintain an inflexible position on it. Secrecy advocates, those who believe that secrecy for government (national security) or corporate (proprietary information) purposes trump the need for transparency, would also likely oppose some or all of the components of this solution. Additionally, transparency advocates, those who fall on the other end of the spectrum, may also oppose this solution as it does provide for a measured/tiered approach (giving the government the ability to address any issues/concerns prior to broader release to the public). To both extremes, secrecy and transparency, this solution may appear as a either falling short (transparency) or going too far (secrecy). This thesis acknowledges the need for secrecy, as well as transparency, and begins by specifically identifying the need for balance between the two, emphasizing the difficulty in weighing whether the “benefits of disclosure outweigh the costs of disclosure" (Stone, 2008). Acknowledging that this is a wicked problem, to which there may be no clear answer, it is all the more apparent that a balanced approach is critical.

The multidisciplinary approach has been used in this solution to provide the checks and balances needed to maintain a balance between secrecy and transparency, without exposing whistleblowers to significant retaliation and consequences. Similar to those safeguards established through the creation of the three U.S. branches of government, creating a whistleblowing process that relies on a partnership between the government and an outside third party ensures accountability, moderation, and flexibility in the application of the solution. With multiple parties and unique perspectives involved in the process, it increases the likelihood of identifying issues and creating innovative solutions. With the rapid evolution of technology, unforeseen possibilities and vulnerabilities, and the ever-changing political environment, rigid adherence to a single process or structure is problematic. Flexibility and adaptability are key components, which must be built into the solution for it to be successful. The spirit of the solution, "facilitating the reporting of wrongdoing while providing protection to whistleblowers," should be the key focus of this process. The details surrounding implementation are peripheral to that central goal, and can (and should) be modified as the environment changes.

B. ALTERNATE FUTURES FOR THE WHISTLEBLOWING ENVIRONMENT

1. Scenario 1: Status Quo

- Congress continues to be torn on the role of whistleblowers in the government, publically supporting whistleblowers, however, unable to enact legislation that provides meaningful protections to government whistleblowers

This scenario is representative of the status quo, and reflects the current atmosphere for both public perceptions and congressional decisions. While whistleblowers have generally been viewed favorably, the incident surrounding the unauthorized disclosures through Wikileaks has created an association of whistleblowers as leakers/traitors, which is evident in the Obama Administration's prosecution of government whistleblowers, as well as the inability of Congress to pass any revised whistleblower bills (whether increasing or decreasing protections).

The solution proposed by this thesis fits very well into this scenario, and could be implemented as a bi-partisan, balanced solution to the problem. It would fit into the agenda for secrecy advocates by potentially reducing the number of unauthorized disclosures (to Wikileaks, Openleaks, etc.), while creating processes to improve and increase transparency in government affairs, a clear goal of transparency advocates.

2. Scenario 2: Increased Protections for Whistleblowers

- Congress changes its position and fully supports whistleblower protections, enacting legislation that encourages whistleblowers (through incentives/protections), clarifies judicial interpretations of the law, creates a user-friendly process for submission and review, and imposes severe penalties in cases of retaliation

This scenario represents a significant shift in the mindset of the U.S. Government, which has historically erred on the side of secrecy over transparency (in actions if not words). If the U.S. Government were to take a definitively pro-whistleblower stance, including carefully worded legislation (to overcome judicial interpretations), significant allocation of resources and authorities to whistleblower protection agencies/organizations, and zero-tolerance for retaliation and reprisals, the whistleblowing environment may radically change over-time.

In this scenario, because of the positive actions of the U.S. Government, many of the concerns addressed by the proposed solution would vanish. The business process and its associated technological components would still be useful and function as a vehicle to facilitate whistleblower reporting; however, the protections provided by anonymity would be redundant.

3. Scenario 3: Decreased Protections for Whistleblowers

- Congress changes its position and associates whistleblowers with traitors/leakers, cracks down on whistleblower protections, and encourages harsh punishments for whistleblowing

This scenario builds upon the negative perceptions generated by the unauthorized disclosures of classified information, the association of whistleblowers as disloyal (rats), and the prosecutions of whistleblowers by the Obama Administration. The result is that Congress not only overturns current whistleblower protections, but also associates whistleblowing with traitors, establishes severe punishments for whistleblowing and strips resources away from agencies responsible to investigate claims of retaliation and reprisal, which could have a stifling effect on the whistleblowing environment, with the number of authorized whistleblowing reports decreasing significantly.

In this scenario, because of the overwhelmingly negative perception of whistleblowing, the solution proposed by this thesis is unlikely to be implemented by the U.S. Government. However, it does seem likely (particularly based on the response of the Internet to legislation, such as the Stop Online Piracy Act (SOPA)) that a similar solution would be developed outside of the government, and organizations, such as Wikileaks would likely see a significant, if not exponential, increase in activity on their site (Greenberg, 2011).

Of all three of these scenarios, the solution proposed by this thesis is best suited to address the current whistleblowing environment, as it provides a balanced approach that can appeal to both secrecy and transparency advocates. If a shift occurs to either of the two extremes, the rationale for and/or likelihood of implementation decreases significantly. With the understanding that the political winds can shift rapidly in either direction, any of these scenarios is possible. If a near-term implementation of the proposed solution occurs, it can be adapted or modified as needed for future scenarios, at little cost.

If implemented, regardless of the future environment, this solution will most likely result in one of the following outcomes.

- Increased authorized whistleblowing, and decreased unauthorized whistleblowing
- Increased authorized whistleblowing, and no effect on unauthorized whistleblowing

- No effect on authorized whistleblowing, and decreased unauthorized whistleblowing
- No effect on the whistleblowing environment (authorized or unauthorized)

It is possible, albeit unlikely, that one of the following outcomes could occur.

- Increased authorized whistleblowing, and increased unauthorized whistleblowing
- Decreased authorized whistleblowing, and increased unauthorized whistleblowing
- No effect on authorized whistleblowing, and increased unauthorized whistleblowing

The top three likely outcomes all reflect positive changes in the whistleblowing environment, with the fourth likely possibility reflecting no change at all. Logically, the three bottom outcomes are unlikely to occur based from the implementation of this solution (they are more likely to result from other factors affecting the environment). The risks associated with implementing this solution, to include cost and the sharing of responsibility for secrecy/transparency with a third party are manageable, and potentially, offset through funding recovered from fraud/waste cases, and through appropriate administration/investigation of whistleblower reports.

C. FUTURE RESEARCH

A few areas of future research should be explored prior to the development and implementation of the recommendations in this thesis.

- **Evaluation of third-party organizations—**To provide for the maximum possibility of success, an appropriate third party must be identified. Only an organization that meets the criteria identified above will be able to provide the credibility required to increase public trust in the process. If the process is not trusted, it will fail.
- **Identification of appropriate investigators—**Currently, multiple avenues exist that whistleblowers can use to submit reports, including the IG, the GAO, and the OSC. Clear roles and responsibilities need to be established that identify appropriate tier one and tier two investigators, and ensure that the investigation process itself meets or exceeds required standards.

- **Analyze and determine appropriate funding levels—**Many of the problems facing government agencies with the responsibility for investigation stem from the lack of appropriate funding and staffing levels, which leads to unacceptable delays and backlogs of investigations, contributing to unauthorized disclosures. Any investigators must have the funding and staffing levels commiserate with the quantity of reports submitted. To reduce stovepiping and backlogs in individual organizations, perhaps partnerships could be formed within tier one and tier two investigators to distribute the workload evenly and reduce the probability of backlogs.
- **Develop metrics for post-implementation evaluation—**While multiple potential outcomes have been identified, the only way to determine success will be through the development of clear metrics, which can be used to evaluate the process, identify its impact on the whistleblowing environment, and prompt changes as needed to support the realization of success.

While this thesis has presented a solution based on a realistic need, clearly identified benefits, and few risks, it is important to understand one last fundamental element required for this solution to be realistically implemented. Regardless of the environment, this solution requires a champion within the government who has the vision, authority and resources to make this happen. This solution cannot be driven from the program manager level of government; it must stem from leadership and contain the authorities and resources necessary for implementation (initially for a pilot program, and ultimately, broader implementation and sustainment). However, by creating an authorized process through which homeland security employees can submit whistleblowing information without fear of reprisals, it may increase the likelihood of whistleblower reporting in the first place, and reduce the number of leaks to unauthorized recipients, which would function as a check and balance system, helping to bypass administrative roadblocks and providing a mechanism through which homeland security can monitor and increase efficiency in its operations.

Despite the efforts of the U.S. Government and its allies, including private sector interests and powerful corporations, Wikileaks continues to demonstrate relevance and operational functionality, most recently through the release of over four million emails from the private security company “Stratfor” (Kelly, 2012). While these emails do not represent whistleblowing (they were hacked by representatives of the Internet organization Anonymous), they do serve to demonstrate further the value of the protection and distribution methods provided through the ‘Wikileaks model.’ Reva Bhalla, the Director of Analysis for Stratfor recently stated, “Wikileaks itself may struggle to survive but the idea that’s put out here, that anyone with the bandwidth and servers to support such a system can act as a prime outlet of leaks. [People] are obsessed with this kind of stuff. The idea behind it won’t die” (Dorling, 2012). The DHS has an opportunity to build upon and improve the “Wikileaks Model,” to harness its use of technology and process to create a solution that would meet the needs of both whistleblowers and the government.

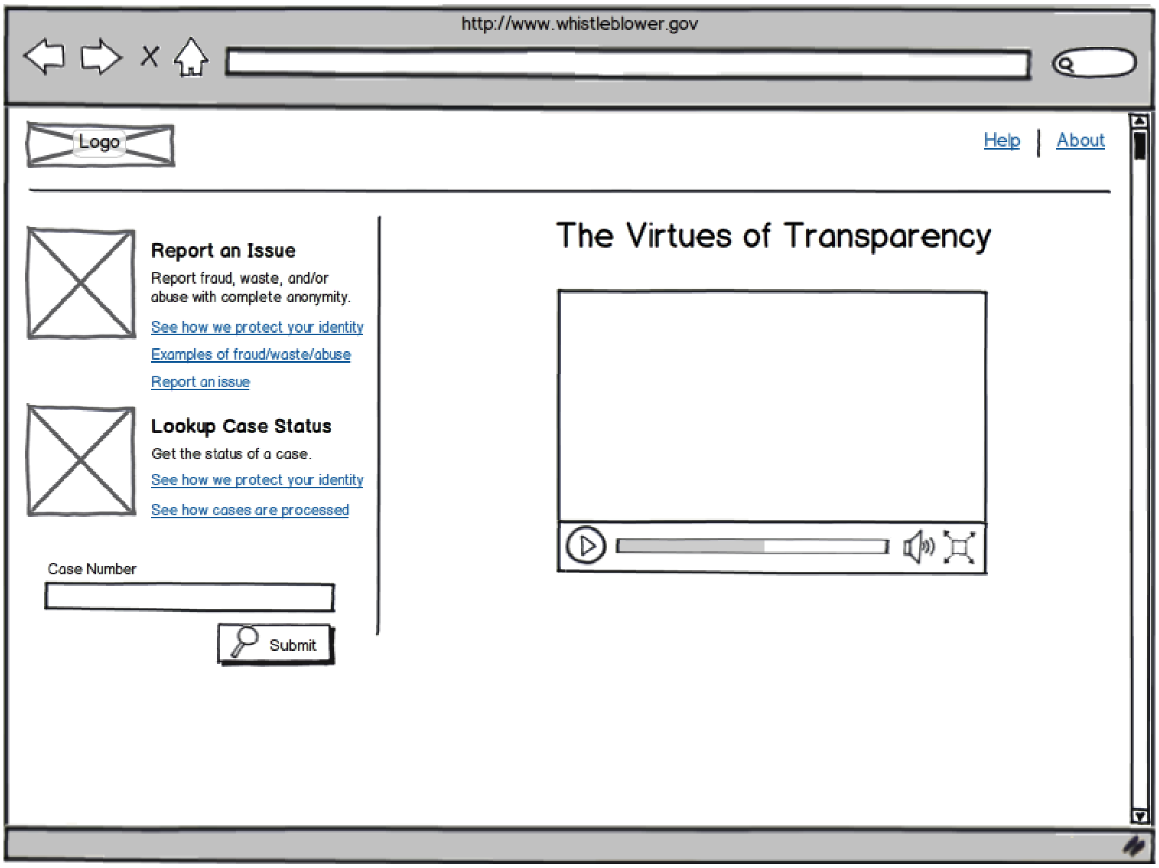
The world is constantly changing, secrets are becoming harder to maintain and democracy is happening in real time via the Internet around the world. The current mentality around whistleblower protection is inadequate, and inaction on this front will result in decreasing instances of authorized whistleblowing and increased unauthorized whistleblowing. It is brave people who do the right thing, regardless of personal cost. It is our duty as government officials to protect them, and to encourage accountability, transparency, and ethics in government operations. It is time to adapt our mindset and catch up to the world around us.

> The world we have created is a product of our thinking…it cannot be changed without changing our thinking.
>
> - Albert Einstein

APPENDIX. RESPONSIBLE DISCLOSURE INFORMATION SYSTEM (RDIS) MOCK-UPS

The Responsible Disclosure Information System would serve as the front-end interface for whistleblowers to access the DHS's responsible disclosure process. The RDIS would allow whistleblowers to submit reports, receive notifications, provide updates, and request escalation, all with relative anonymity. The following nine screen shots serve as an example of what the RDIS might look like, and allow for a little more in-depth view of the system itself.

Welcome Page


http://www.whistleblower.gov
Logo
Help | About
The Virtues of Transparency
Report an Issue
See how we protect your identity
Examples of fraud/waste/abuse
Report an issue
Lookup Case Status
See how we protect your identity
See how cases are processed
Case Number
Submit

Report fraud, waste, and/or abuse with complete anonymity.

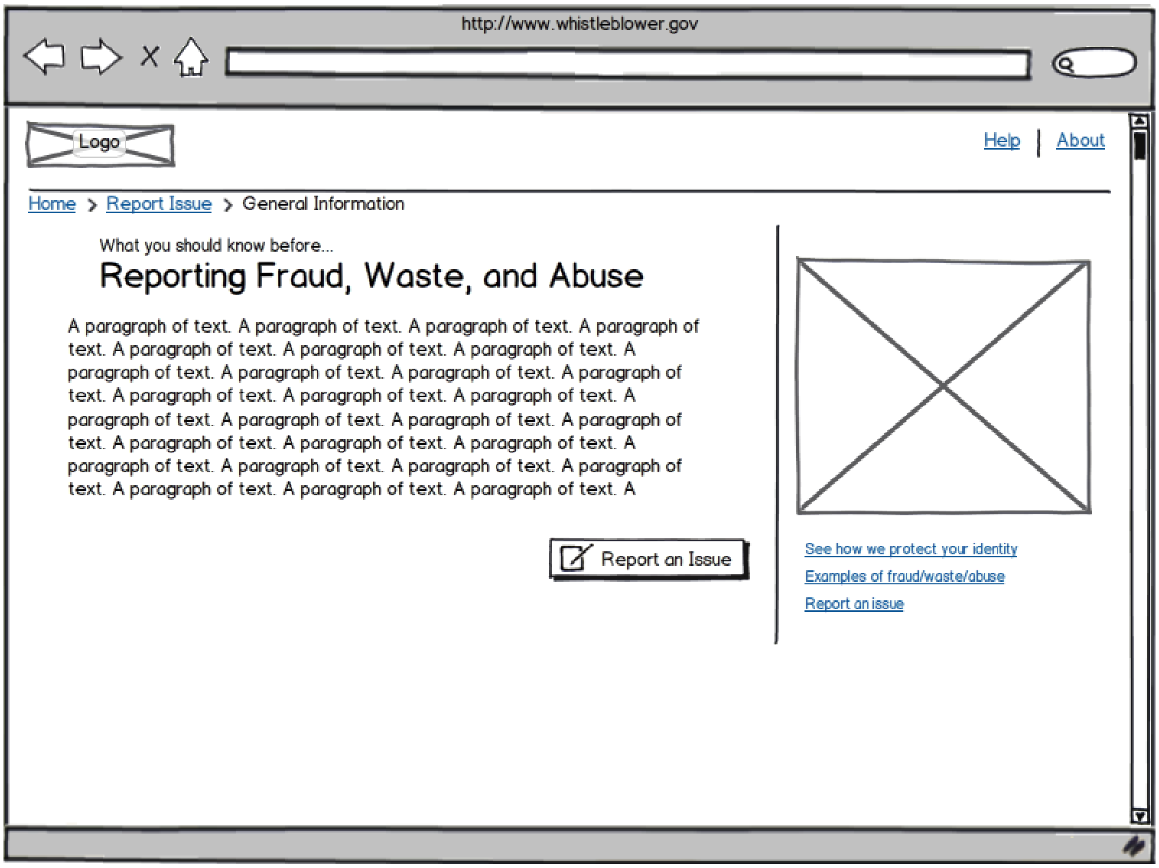
Get the status of a case.

This introductory page would serve as the main page for the RDIS. On the right would be a welcome/background video given by a senior DHS official, reinforcing the legitimacy and importance of this process, and the role of whistleblowers in government.

From this page, users would be able to follow links to:

- General/background information
- Submit a report
- Lookup a case (previously submitted report)

General Information


http://www.whistleblower.gov
Logo
Help | About
Home > Report Issue > General Information
Report an Issue
See how we protect your identity
Examples of fraud/waste/abuse
Report an issue

What you should know before...

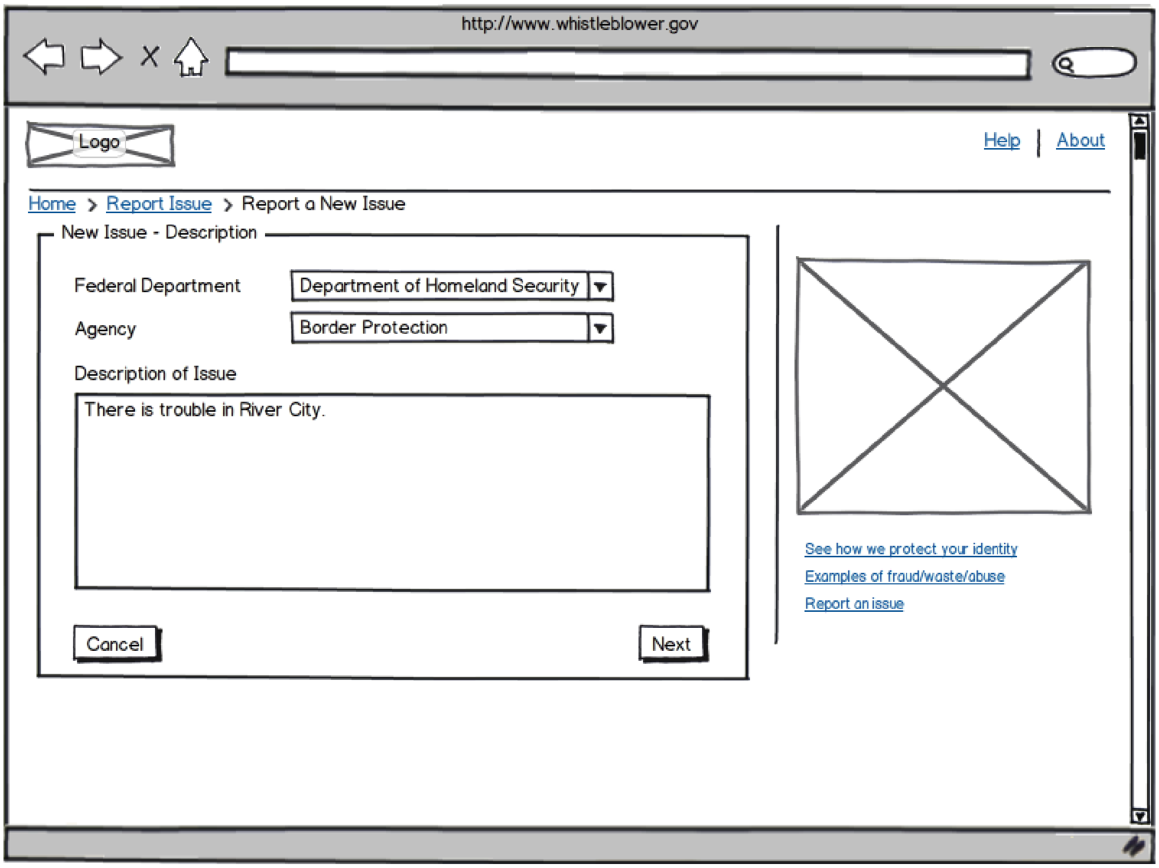
Reporting Fraud, Waste, and Abuse

A paragraph of text. A

This general/background information page would serve to provide users additional details to help users make informed decisions. This page is designed to assist employees who have already decided to become whistleblowers, those who are considering their options, as well as to educate other employees on the appropriate process. This page provides information on the following.

- The definition of organizational wrongdoing and examples
- A detailed explanation of the Responsible Disclosure Process
- Details on the protections offered by the RDIS and the limitations associated with the process
- Recommendations for practicing ‘good hygiene’ as whistleblowers

Report an Issue: Event Description



http://www.whistleblower.gov
Logo
Help | About
Home > Report Issue > Report a New Issue
New Issue - Description
See how we protect your identity
Examples of fraud/waste/abuse
Report an issue
Cancel
Next

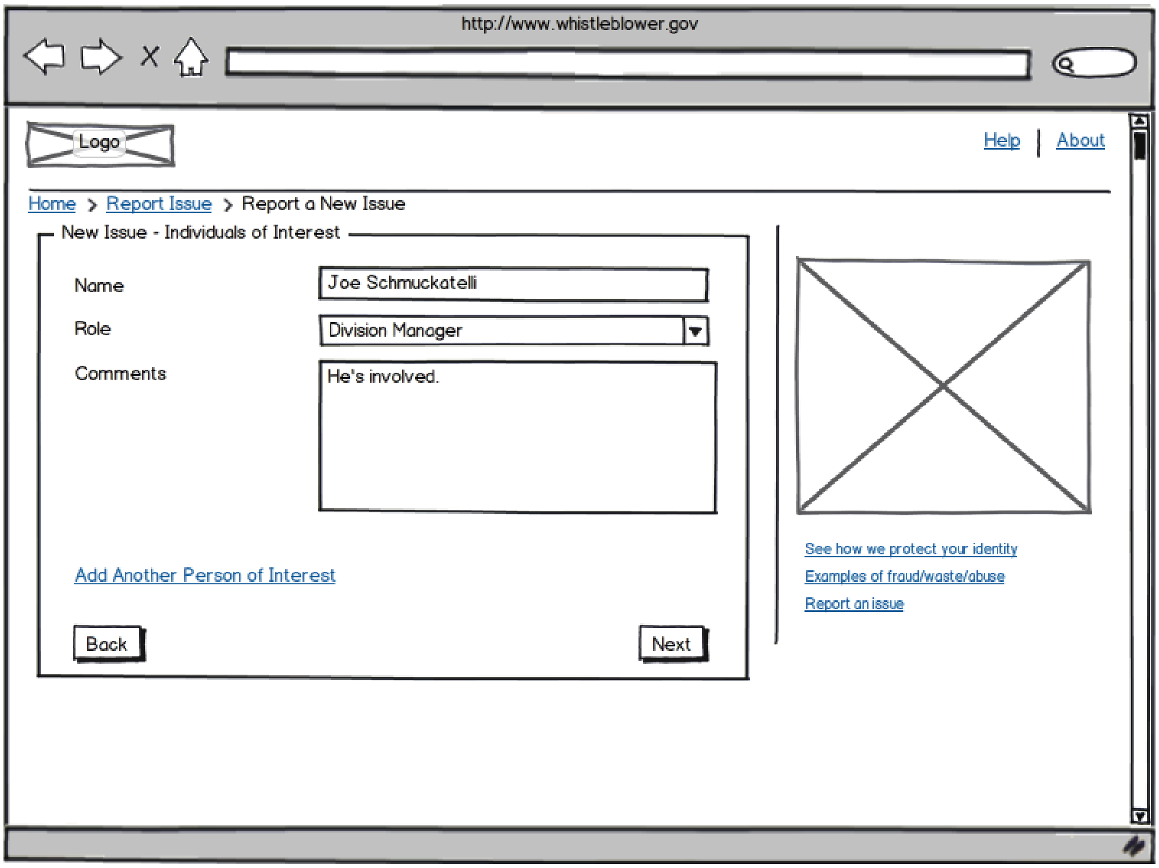
Federal Department: Department of Homeland Security

Agency: Border Protection

Description of Issue: There is trouble in River City.

This page is the first page of the submission process. The whistleblower would provide the initial report on the issue, identifying the agency, suspected wrongdoing, and additional pertinent information.

Report an Issue: Event Description



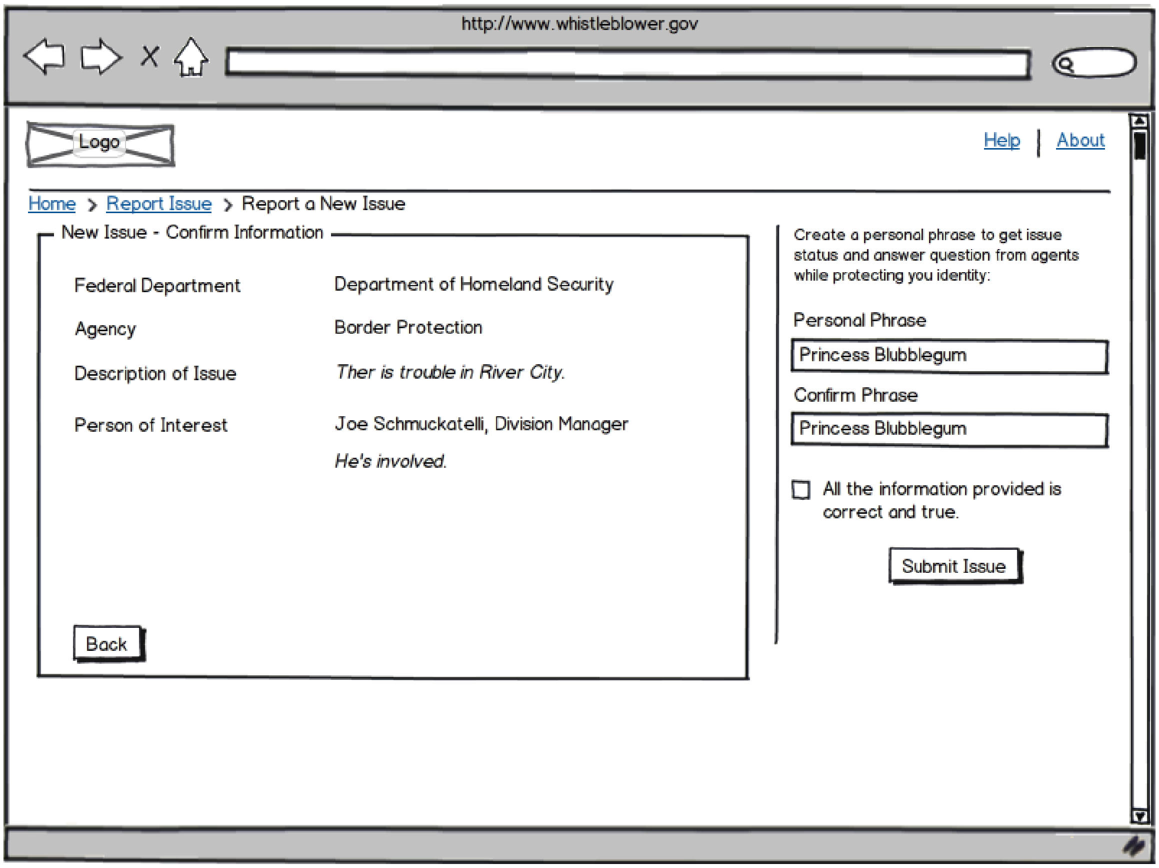
http://www.whistleblower.gov
Logo
Help | About
Home > Report Issue > Report a New Issue
See how we protect your identity
Examples of fraud/waste/abuse
Report an issue
Add Another Person of Interest
Back
Next

New Issue - Individuals of Interest

Name	Joe Schmuckatelli
Role	Division Manager
Comments	He's involved.

This page is the second page of the submission process. The whistleblower could submit the names of individuals; either those directly involved or people who may be able to provide additional information during the investigation.

Report an Issue: Review and Submissions



http://www.whistleblower.gov

Home > Report Issue > Report a New Issue

New Issue - Confirm Information

Federal Department	Department of Homeland Security
Agency	Border Protection
Description of Issue	*Ther is trouble in River City.*
Person of Interest	Joe Schmuckatelli, Division Manager *He's involved.*

Create a personal phrase to get issue status and answer question from agents while protecting you identity:

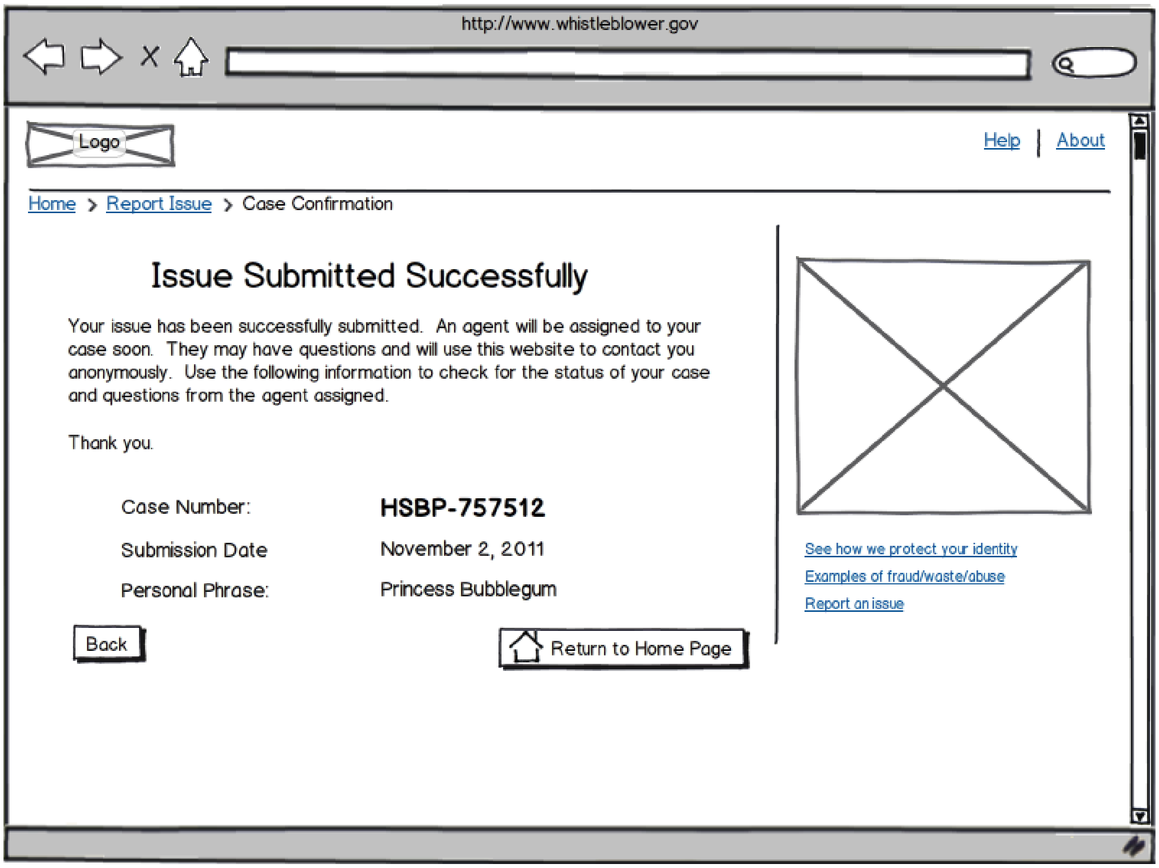
Personal Phrase: Princess Blubblegum

Confirm Phrase: Princess Blubblegum

□ All the information provided is correct and true.

This is the final page of the submission process. The whistleblower would review the information to ensure accuracy prior to submission and also create a ‘personal passphrase’ to allow to access case files on the RDIS in the future.

Case Confirmation



http://www.whistleblower.gov
Logo
Help | About
Home > Report Issue > Case Confirmation

Issue Submitted Successfully

Your issue has been successfully submitted. An agent will be assigned to your case soon. They may have questions and will use this website to contact you anonymously. Use the following information to check for the status of your case and questions from the agent assigned.

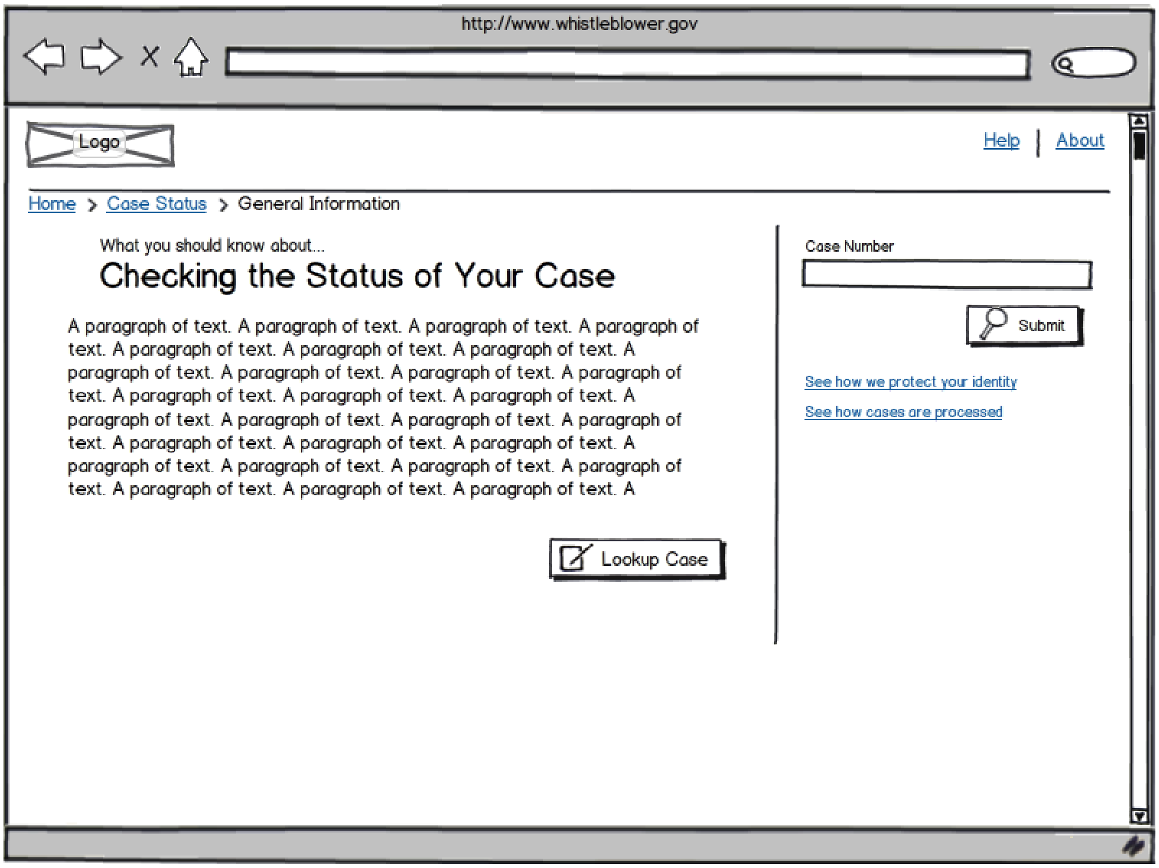
Thank you.

Case Number:	**HSBP-757512**
Submission Date	November 2, 2011
Personal Phrase:	Princess Bubblegum

Back
Return to Home Page
See how we protect your identity
Examples of fraud/waste/abuse
Report an issue

This page is the confirmation page for submission of the whistleblower’s report. It is important for whistleblowers to record the information here, as all three items (case number, submission date, and personal phrase) are required to access case files in the future.

Case Lookup: General Information


http://www.whistleblower.gov
Logo
Help
About
Home
Case Status
General Information
Lookup Case
Case Number
Submit
See how we protect your identity
See how cases are processed

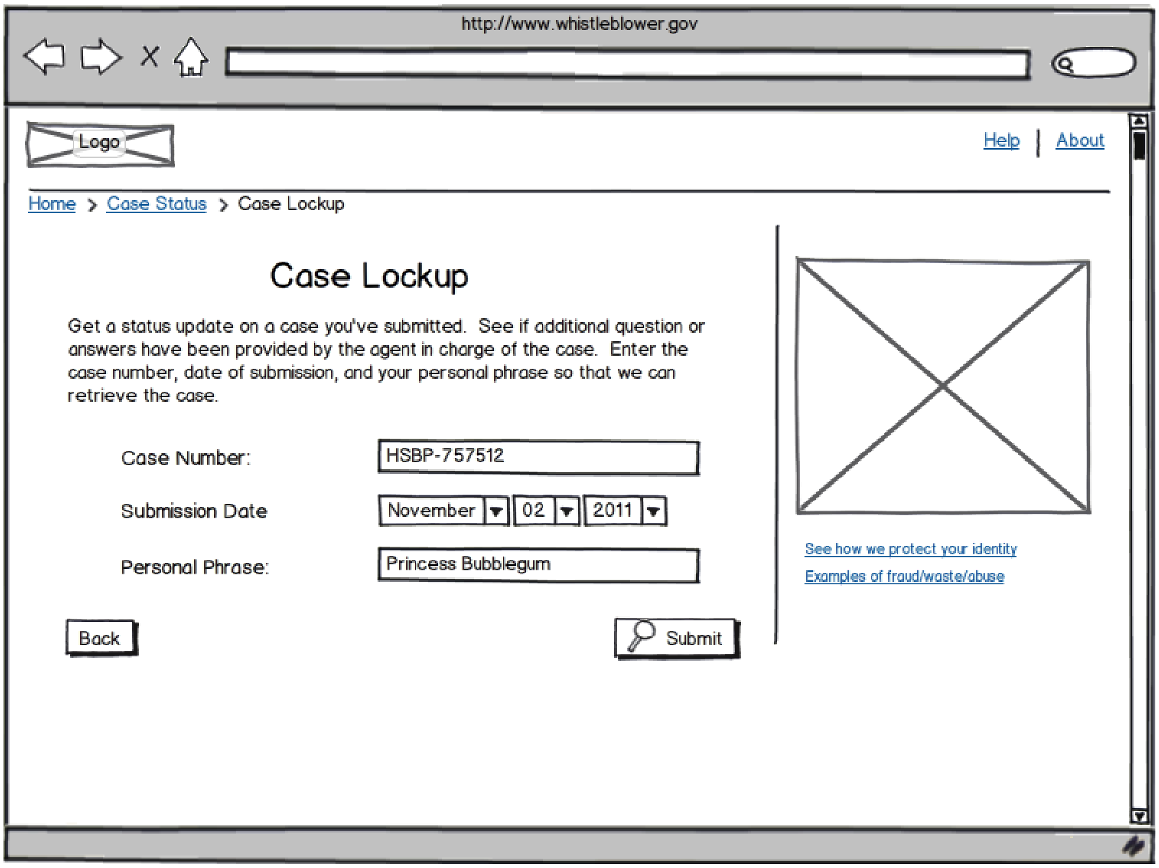
What you should know about...

Checking the Status of Your Case

A paragraph of text. A

Upon completion of the submission process, RDIS users would be directed to this case lookup information page, which would provide additional information about the process, specifically the investigation timelines, roles and responsibilities, and personal protections of which whistleblowers should be aware. Whistleblowers are also informed of when they should check into the RDIS for updated information, and the possible actions they can take in the future.

Case Lookup: *Request*


http://www.whistleblower.gov
Logo
Help | About
Home > Case Status > Case Lockup
See how we protect your identity
Examples of fraud/waste/abuse
Back
Submit

Case Lockup

Get a status update on a case you've submitted. See if additional question or answers have been provided by the agent in charge of the case. Enter the case number, date of submission, and your personal phrase so that we can retrieve the case.

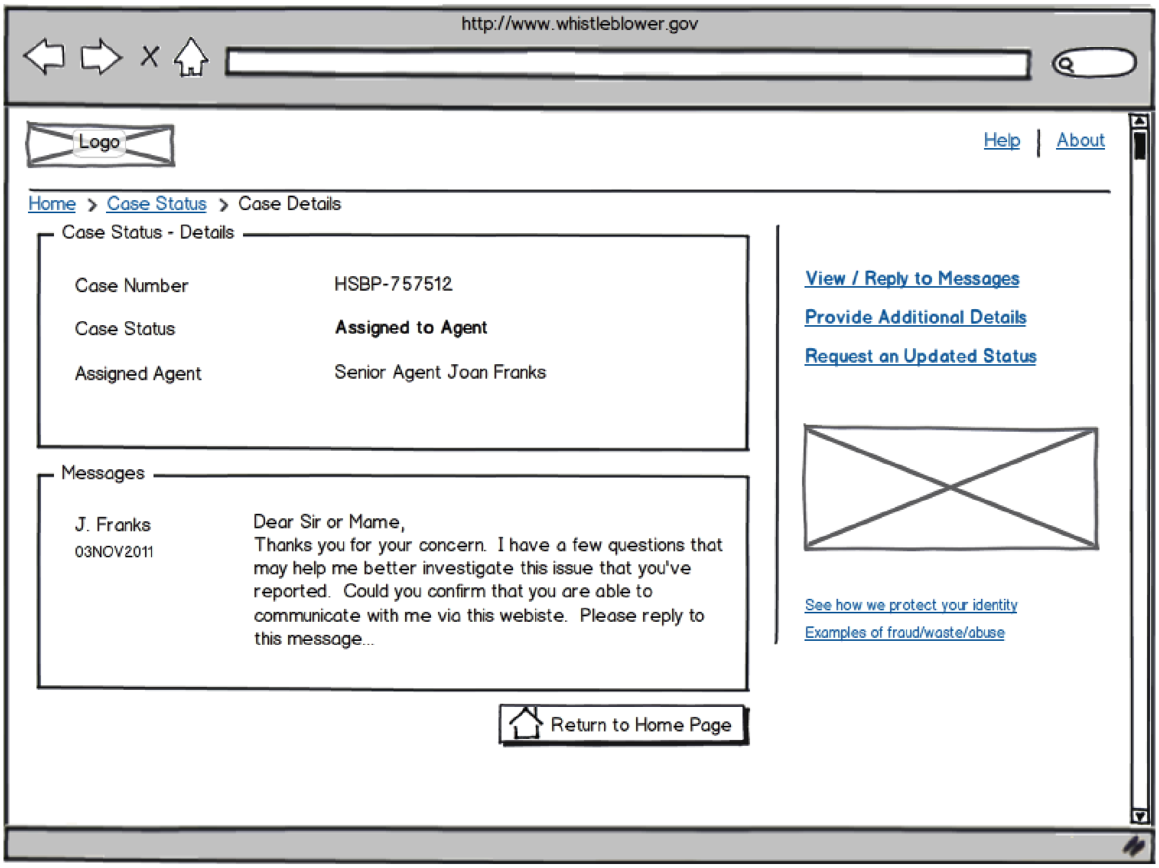
Case Number: HSBP-757512

Submission Date: November ▾ 02 ▾ 2011 ▾

Personal Phrase: Princess Bubblegum

At defined intervals during the Responsible Disclosure process, the RDIS will be updated with information on the status of the case. Through this page, whistleblowers can access the case status/message page by providing the case number, submission date, and personal phrase generated upon their initial submission.

Case Lookup: *Case Details*


http://www.whistleblower.gov
Logo
Help | About
Home > Case Status > Case Details
View / Reply to Messages
Provide Additional Details
Request an Updated Status
See how we protect your identity
Examples of fraud/waste/abuse
Return to Home Page

Case Status - Details

Case Number	HSBP-757512
Case Status	**Assigned to Agent**
Assigned Agent	Senior Agent Joan Franks

Messages

J. Franks
03NOV2011

Dear Sir or Mame,
Thanks you for your concern. I have a few questions that may help me better investigate this issue that you've reported. Could you confirm that you are able to communicate with me via this webiste. Please reply to this message...

This case lookup page will provide the whistleblower information on the current status of their case. It also includes a messaging function, a vehicle through which investigators/coordinators can request or receive information from whistleblowers (who retain anonymity).

LIST OF REFERENCES

A Web of English History. (2009, September 29). *John Wilkes*. Retrieved from A Web of English History website: http://www.historyhome.co.uk/people/wilkes.htm

Addley, E. (2011, December 5). *Julian Assange extradition fight to continue in supreme court*. Retrieved from The Guardian UK website: http://www.guardian.co.uk/media/2011/dec/05/julian-assange-extradition-fight-supreme-court?INTCMP=ILCNETTXT3487

Aftergood, S. (2009, July 29). *More than 2.4 million hold security clearances*. Retrieved from Secrecy News website: http://www.fas.org/blog/secrecy/2009/07/security_clearances.html

Aftergood, S. (2010a). *Wikileaks fails 'due diligence' review*. Retrieved from Federation of American Scientists website: http://www.fas.org/blog/secrecy/2010/06/wikileaks_review.html

Aftergood, S. (2010b). *Telling secrets*. Retrieved from Foreign Policy website: http://www.foreignpolicy.com/articles/2010/10/15/telling_secrets?page=0,0

Agrell, W. (2002, October). *When everything is intelligence—Nothing is intelligence* . Retrieved from Central Intelligence Agency Library website: https://www.cia.gov/library/kent-center-occasional-papers/vol1no4.htm

Akdeniz, Y. (2002). Anonymity, democracy, and cyberspace. *Social Research*, 223–237.

AnonWatch. (n.d.) Retrieved from http://www.anonwatch.com/proxy/

Anonymizer. (n.d.). Retrieved from http://www.anonymizer.com

Assange, J. (2009, July). *Why the world needs Wikileaks*. Retrieved from TED: Ideas Worth Spreading website: http://www.ted.com/talks/julian_assange_why_the_world_needs_wikileaks.html

Assange, J. (2010, July 26). WikiLeaks founder Julian Assange on the 'war logs': 'I enjoy crushing bastards'. (J. a. Goetz, Interviewer)

Associated Press. (2010, July 26). Wikileaks whistle-blower website publishes 91K classified documents on Afghan war. Retrieved from New Jersey Online website: http://www.nj.com/news/index.ssf/2010/07/website_publishes_91k_classifi.html

Baker, R. (2010, July 28). *Its wikitreason and its deadly*. Retrieved from NY Daily News website: https://www.nydailynews.com/opinions/2010/07/28/2010-07-28_its_wikitreason_and_its_deadly_dont_minimize_the_damage_julian_assange_has_done.html?obref=obnetwork

Banisar, D. (2007). *Government secrecy: Decisions without democracy.* Washington, DC: People for the American Way.

Barret, V. M. (2007, October 15). *Anonymity & the net*. Retrieved from Forbes website: http://www.forbes.com/forbes/2007/1015/074.html

Baxter, B. (2010, July 27). *Privaledged information in a Wikileaks world*. Retrieved from Law website: http://www.law.com/jsp/article.jsp?id=1202463926368&Privileged_Information_in_a_WikiLeaks_World

Bellavita, C. (2011, December 20). *A new perspective on homeland security?* Retrieved from Homeland Security Watch website: http://www.hlswatch.com/2011/12/20/a-new-perspective-on-homeland-security/

Bennington, J., & King, R. H. (2010). *Perception on social networking: A study on their operational relevance for the Navy* (master's thesis). Naval Postgraduate School, Monterey, CA.

Blaze, M. F. (1996). *Decentralized trust management.* Murray Hill, NJ: AT&T Research.

Blodget, H. (2010, September 28). *Wikileaks spokesman quits*. Retrieved from Business Insider website: http://www.businessinsider.com/wikileaks-spokesman-quits

Bovens, M. (2005). Public accountability. In *The Oxford Handbook of Public Management* (pp. 182–207).

Boyd, C. (2010, July 27). *WikiLeaks tech challenges 'top secret' security*. Retrieved from Discovery News website: http://news.discovery.com/tech/wikileaks-tech-challenges-top-secret-security.html

Clark, D. D. (2010). The problem isn't attribution: it's multi-stage attacks. *ReARCH'10 Proceedings of the Re-Architecting the Internet Workshop*. New York: ACM.

Committee on Government Reform, House of Representatives. (2006). *National security whistleblowers in the post-September 11th era: Lost in a labyrinth and facing subtle retaliation.* Washington, DC: U.S. Government Printing Office.

Continental Congress. (1778, July 30). *Journals of the Continental Congress, 1774–1789*. Retrieved from American Memory website: http://memory.loc.gov/cgi-bin/query/r?ammem/hlaw:@field%28DOCID+@lit%28jc01172%29%29

The Constitution Project's Liberty and Security Committee. (2009). *Reining in excessive secrecy: Recommendations for reform of the classification and controlled unclassified information systems.* Washington, DC: The Constitution Project.

Council of Europe—Committe on Legal Affairs and Human Rights. (2008). *The protection of "whistleblowers."* Parliamentary Assembly—Council of Europe.

Covey, S. M. (2006). *The speed of trust* . New York, NY: Free Press.

Cryptome. (n.d.). Retrieved from Cryptome: http://cryptome.org/

Cusak, A. (2011, April 17). *The mornings of the world*. Retrieved from http://www.andrewcusack.com/2011/04/17/the-mornings-of-the-world/

Davenport, D. (2002). Anonymity on the Internet: Why the price may be to high. *Communications of the ACM,* 33–35.

Democracy Now. (2008, April 1). *Exposing the NSA's warrantless wiretapping program*. Retrieved from You Tube website: http://www.youtube.com/watch?v=BPx8nomoYTk

Deparment of Defense. (n.d.). *About the DoD hotline*. Retrieved from Department of Defense Hotline website: http://www.dodig.mil/HOTLINE/

Department of Defense Inspector General. (2007, December 17). *Instruction for defense hotline program*. Washington, DC: Department of Defense.

Department of Health and Human Services. (2011, December 13). *News release*. Retrieved from http://www.hhs.gov/news/press/2011pres/12/20111213a.html

Devine, S. (2010). *Whistleblower witch hunts: The smokescreen syndrome.* Washington, DC: Government Accountability Project.

Devine, T. (2011, January 10). *Who killed the whistle-blower bill?* Retrieved from Los Angeles Times website: http://articles.latimes.com/2011/jan/10/opinion/la-oe-devine-whistleblower-20110110

Diamond, L. (2010). Liberation technology. *Journal of Democracy*, 69–83.

Domscheit-Berg, D. S. (2010, September 27). Wikileaks spokesman quits: The only option left for me is an orderly departure. (M. Rosenbach, Interviewer) *Der Spiegel Online.*

Dorling, P. (2012, February 29). *Revealed: US plans to charge Assange*. Retrieved from The Syndey Morning Herald website: http://www.smh.com.au/technology/technology-news/revealed-us-plans-to-charge-assange-20120228-1u14o.html

Duke Law. (n.d.). *Supreme court online: Garcetti v. Ceballos*. Retrieved from http://www.law.duke.edu/publiclaw/supremecourtonline/certgrants/2005/garvceb.html

Egelko, B. (2006, May 7). *The Balco case/More pressure on reporters to name sources*. Retrieved from SFGate website: http://articles.sfgate.com/2006-05-07/news/17297014_1_new-york-times-reporter-prosecutors-government-secrecy

Facebook: About us. (n.d.). Retrieved from http://www.facebook.com/facebook

Fakhoury, H. (2011, June 7). *WSJ and Al-Jazeera lure whistleblowers with false promises of anonymity*. Retrieved from The Electronic Frontier Foundation website: https://www.eff.org/deeplinks/2011/06/wsj-and-al-jazeera-lure-whistleblowers-false

Fisher, L. (2005, December 30). *National security whistleblowers.* (Congressional Report No. RL3321). Washington DC: Library of Congress Congressional Research Service.

Franklin, M. K. (1997). *Fair exchange with a semi-trusted third party*. Murray Hill, NJ: ACM.

Gamble, M. (2011, December 19). *False claims recoveries and whistleblower suits reach all-time high*. Retrieved from Becker's ASC Review website: http://www.beckersasc.com/stark-act-and-fraud-abuse-issues/false-claims-recoveries-and-whistleblower-suits-reach-all-time-high.html

Giddens, A. (1990). *The consequences of modernity.* Cambridge: Polity Press.

GoldenFrog. (n.d.). VyprVPN. Retrieved from https://www.goldenfrog.com/vyprvpn

Goodman, M. C. (2007). *Disavowed: The government's unchecked retaliation against national security whistleblowers.* New York: American Civil Liberties Union.

Government Accountability Office. (2009, March 30). *GAO seeks the public's help in fighting waste, fraud, abuse or mismanagement of recovery act funds*. Washington, DC: Government Accountability Office.

Government of the United Kingdom. (1998). *Public Interest Disclosure Act 1998.* Retrieved from Legistlation.gov.uk: http://www.legislation.gov.uk/ukpga/1998/23/contents

Grassley, C. (2004, July 17). *Senators concerned about more alleged problems at FBI's office of professional responsibility*. Retrieved from http://grassley.senate.gov/releases/2004/p04r07-14.htm

Greenberg, A. (2011, November 23). *Wary of SOPA, Reddit users aim to build a new, censorship-free internet*. Retrieved from Forbes website: http://www.forbes.com/sites/andygreenberg/2011/11/23/wary-of-sopa-reddit-users-aim-to-build-a-new-censorship-free-internet/

Greenwald, G. (2010, April 16). *What the whistleblower prosecution says about the Obama DOJ*. Retrieved from The New York Times website: http://www.salon.com/news/opinion/glenn_greenwald/2010/04/16/prosecutions

Griffith University. (n.d.). *Whistling while they work*. Retrieved from http://www.griffith.edu.au/criminology-law/whistleblowing

Guth, D. W. (2008). *Untapped potential: Evaluating state emergency management agency web sites 2008*. Lawrence: University of Kansas Transportation Research Institute.

Hall, H. T. (2005). *Exploring the relationship between U.S. government secrecy and democracy: Classification, cultures of secrecy and the public sphere.* Norman: University of Oklahoma.

Hermann, D. W. (2009). Proceedings of the 2009 ACM Workshop on Cloud Computing Security*: Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies With Multinomial Naive-Bayes Classifiers*. ACM.

Hide your IP address with a VPN. (2011). Retrieved from http://www.hideyourselfonline.com/vpn.htm

Hoffman, D. L. (1999). Building consumer trust online. *Communications of the ACM* .

Hsu, S. S. (2011, February 3). *Bush whistleblower prosecutor faces jail*. Retrieved from Washington Post website: http://www.washingtonpost.com/wp-dyn/content/article/2011/02/03/AR2011020303180.html

I2P. (n.d.). I2P Anonymous network. Retrieved from http://www.i2p2.de/index.html

Johnson, R. A. (2003). *Whistleblowing: When it works and why.* Boulder: Lynne Rienner Publishers, Inc.

JonDonym. (n.d.). http://anonymous-proxy-servers.net/

Jones, J. M. (2010, December 15). *Congress' job approval rating worst in Gallup history*. Retrieved from Gallup website: http://www.gallup.com/poll/145238/congress-job-approval-rating-worst-gallup-history.aspx

Kelly, M. (2012, February 27). *Wikileaks to publish Stratfor hack e-mails, the firm responds*. Retrieved from VentureBeat News website: http://venturebeat.com/2012/02/27/stratfor-wikileaks-emails/

Knight, P. (2010, December 15). *American grocers*. Retrieved from Houston Press website: http://www.houstonpress.com/2010-12-16/news/american-grocers/

Kohn, S. M. (2011). *The whistleblower's handbook.* Guilford: Lyons Press.

Kosar, K. R. (2009, December 31). *Security classification policy and procedure: E.O. 12958, as amended.* (Congressional Report No. 97-771). Washington DC: Library of Congress Congressional Research Service.

Kosar, K. R. (2010, December 10). *Classified information policy and executive order 13526.* (Congressional Report No. R4152). Washington DC: Library of Congress Congressional Research Service.

Lajeunesse, W. (2011, November 30). *'Fast and furious' whistleblowers struggle six months after testifying against ATF program*. Retrieved from Fox News website: http://www.foxnews.com/politics/2011/11/30/fast-and-furious-whistleblowers-struggle-six-months-after-testifying-against/

Lee, Y.-C. (2006). Internet and anonymity. *Society*, 5–7.

Leigh, D. (2010, October 14). *WikiLeaks says funding has been blocked after government blacklisting*. Retrieved from The Guardian website: http://www.guardian.co.uk/media/2010/oct/14/wikileaks-says-funding-is-blocked

Lewis, D. B. (2010). *A global approach to public interest disclosure: What can we learn from existing whistleblowing legistlation and research.* Cheltenham: Edward Elgar Publishing.

Lloyd, J. (n.d.). *What media are doing to our politics.* Retrieved from University of Groningen website: http://www.rug.nl/dnpp/lioyd.pdf

Mayer, J. R. (2009, April 7). *"Any person...a pamphleteer" Internet anonymity in the age of web 2.0.* Woodrow Wilson School of Public and International Affairs.

Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008). *Whistleblowing in organizations.* New York: Routledge.

Miethe, T. D. (1999). *Whistleblowing at work.* Boulder: Westview Press.

Mihm, J. C. (2001). *Observations on protections from discrimination and reprisal for whistleblowing.* Washington, DC: Government Accountability Office.

Mixminion: A type III anonymous remailer. (n.d.) Retrieved from http://mixminion.net/

Montalbano, E. (2010, March 16). *Army: Wikileaks a national security threat*. Retrieved from Information Week website: http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=223900094

Moon, J. M. (2003). Proceedings of the 36th Hawaii International Conference on System Sciences: *Can IT Help Government to Restore Public Trust?: Declinine Public Trust and Potential Prospects of IT in the Public Sector*. (p. 8). Washington, DC: IEEE Computer Society.

Morrison, A. (2005). Some things, you're better off not knowing...Thoughts on ratemyprofessors.com. *English Studies in Canada*, 16–21.

National Commision On Terrorist Attacks Upon The United States. (2004). *The 9/11 commission report.* New York: W.W. Norton & Company.

National Whistleblowers Center. (2010). *Fighting fraud*. Retrieved from National Whistleblowers Center: http://www.whistleblowers.org/index.php?option=com_advancedtags&view=tag&id=80

Nystedt, D. (2009, October 9). *Wikileaks plans to make the world a leakier place*. Retrieved from Computer World website: http://www.computerworld.com/s/article/9139180/Wikileaks_plans_to_make_the_Web_a_leakier_place

Office of the White House Press Secretary. (2009, December 29). *Executive order—Classified national security information*. Retrieved from http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

O'Keefe, E. (2009, January 21). *New Obama orders on transparency, FOIA requests*. Retrieved from The Washington Post website: http://www.google.com/#hl=en&sugexp=ldymls&xhr=t&q=Obama+foia+policy&cp=12&pf=p&sclient=psy&rlz=1R2SKPT_enUS399&aq=0&aqi=&aql=&oq=Obama+foia+p&pbx=1&bav=on.2,or.&fp=ee7ae51cefa9981c

Onion Routing. (n.d.). http://www.onion-router.net/

The Parliament of the Commenweath of Australia. (2007). *Public interest disclosures bill 2007*. Retrieved from Commonwealth of Australia Bills website: http://www.austlii.edu.au/au/legis/cth/bill/pidb2007323/

Parent, M. (2005). Building citizen trust through e-government. *Government Information Quarterly*, 720–736.

Pew Research Center. (2011, August 25). *Anger and distrust in government*. Retrieved from http://people-press.org/2011/08/25/section-4-anger-and-distrust-in-government/

Polania, W. G. (2010). *Leveraging social networking technologies: An analysis of the knowledge flows facilitated by social media and the potential improvements in situational awareness, readiness, and productivity* (master's thesis). Naval Postgraduate School, Monterey, CA.

Project on Government Oversight, Government Accountability Project, Public Employees for Environmental Responsibility. (2002). *The art of anonymous activism; Serving the public while surviving public service.* Washington, DC: Project on Government Oversight, Government Accountability Project, Public Employees for Environmental Responsibility.

Project on Government Oversight. (2005, April 28). *Homeland and national security whistleblower protections: The unfinished agenda*. Retrieved from http://www.pogo.org/pogo-files/reports/whistleblower-issues/the-unfinished-agenda/#14

Public Concern At Work. (2010, March). *Where's whistleblowing now?* Retrieved from http://www.google.com/url?sa=t&source=web&cd=1&sqi=2&ved=0CB0QFjAA&url=http%3A%2F%2Fwww.pcaw.co.uk%2Fpolicy%2Fpolicy_pdfs%2FPIDA_10year_Final_PDF.pdf&rct=j&q=Where%27s%20whistleblowing%20now&ei=Y5dITozRL6To0QGvopzIBw&usg=AFQjCNFiOCi2-A7wlRcy_fF-SvzpGTgwyQ

Public Concern At Work. (n.d.). *Public interest disclosure act—Guide to law & practice.* Retrieved from http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBYQFjAA&url=http%3A%2F%2Fwww.pcaw.co.uk%2Flaw%2Flaw_pdfs%2Fpida%2520guide.pdf&rct=j&q=PIDA%20Guide&ei=bpZITtezPKPk0QHcuJmNCA&usg=AFQjCNGt0glcAhp0n85kXs2_9cPHWloHpQ&sig2=_rxXw5nYXTIZQZFFuLXY_Q&cad=rja

Public Proxy Servers. (n.d.) http://www.publicproxyservers.com/

Randomwire. (2011). http://www.randomwire.com/tor

Rashid, F., & Edmondson, A. C. (2011). *Risky trust: How multi-entity teams develop trust in a high risk endeavor.* Boston: Harvard Business School.

Reals, T. (2010, July 28). *WikiLeaks reportedly outs 100s of Afghan informants*. Retrieved from CBS News website: http://www.cbsnews.com/8301-503543_162-20011886-503543.html

The Recorder. (2008, October 16). *Posey V. Lake Pend Oreille School District No. 84*. Retrieved from Law.com website: http://www.law.com/jsp/article.jsp?id=1202425296418&slreturn=1

Reinventing the News Room. (2010, July 26). *A smart play by Wikileaks*. Retrieved from http://reinventingthenewsroom.wordpress.com/2010/07/26/a-smart-play-by-wikileaks/

Romanian Parliament. (2004, December 17). *Romanian Law 571-2004.* Retrieved from Whistleblowing.it website: http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBYQFjAA&url=http%3A%2F%2Fwww.whistleblowing.it%2FRomanian%2520Law%2520571-2004%2520-%2520whistleblowingEN.pdf&rct=j&q=LAW%20No.%20571%20of%2014%20December%202004%20regarding%20the%20protection%20of%20pe

Rosen, J. (2010, July 26). *The Afghanistan war logs released by Wikileaks, the world's first stateless news organization*. Retrieved from Press Think website: http://archive.pressthink.org/2010/07/26/wikileaks_afghan.html

Rosenweig, P. (2010, December 8). *Wikileaks and Julian Assange: Time to update U.S. espionage laws.* Retrieved from The Heritage Foundation website: http://www.heritage.org/research/reports/2010/12/wikileaks-and-julian-assange-time-to-update-us-espionage-laws

Rowley, C. (2010, October 15). *WikiLeaks and 9/11: What if?* Retrieved from The Los Angeles Times website: http://articles.latimes.com/2010/oct/15/opinion/la-oe-rowley-wikileaks-20101015

Saad, L. (2010, January 27). *U.S. news media gets tepid ratings as Obama watchdog*. Retrieved from Gallup website: http://www.gallup.com/poll/125399/news-media-tepid-ratings-obama-watchdog.aspx

Sam Adams Associates for Integrity in Intelligence. (2010, October 24). *Wikileaks and Assange honored*. Retrieved from Truthout website: http://www.truth-out.org/wikileaks-and-assange-honored64545

Schwellenbach, N. (n.d.). *Center for public integrity—Accountability: Anti-whistleblower track record continues*. Retrieved from Government Accountability Project website: http://www.whistleblower.org/press/gap-in-the-news/2009/351

Shenon, P. (2010, July 14). Entering the secret world of Wikileaks. (D. Davies, Interviewer)

Shirky, C. (2009, June). *How social media can make history*. Retrieved from TED: Ideas Worth Spreading website: http://www.ted.com/talks/clay_shirky_how_cellphones_twitter_facebook_can_make_history.html

Shirky, C. (2010, December 31). *Half-formed thought on Wikileaks & global action*. Retrieved from Clay Shirky Weblog: http://www.shirky.com/weblog/2010/12/

Smith, R. (2010). The role of whistle-blowing in governing well: Evidence from the Australian public sector. *The American Review of Public Administration* , 704–721.

Spaulding, S. (2010, June 24). *No more secrets: Then what?* Retrieved from Huffington Post website: http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-what_b_623997.html

Stewart, S. (2010, October 28). *Wikileaks and the culture of classification.* Retrieved STRATFOR website: http://www.stratfor.com/weekly/20101027_wikileaks_and_culture_classification

Stone, G. R. (2008, June). *On secrecy and transparency: Thoughts for Congress and a new administration.* Retrieved from American Constituion Society for Law and Policy website: http://www.acslaw.org/files/Geoff%20Stone%20Issue%20Brief.pdf

StrongVPN. (n.d.). Retrieved from http://strongvpn.com/

Suler, J. (2004). The online disinhibtion effect. *Cyber Psychology and Behavior 7*(3), 321–326.

Symington, A. (2009, September 1). *Exposed: Wikileaks secrets*. Retrieved from Wired UK website: http://www.wired.co.uk/magazine/archive/2009/10/start/exposed-wikileaks-secrets?page=all

Tarbet, G. (2009). *Categorizing a system: Why must this be so hard?* Retrieved from The Compliance Authority website: http://www.thecomplianceauthority.com/categorizing-a-system.php

Tolbert, C. (2006). The effects of e-government on trust and confidence in government. *Public Administration Review,* 354–369.

Tor. (n.d.a.). https://www.torproject.org/

Tor. (n.d.b.). Tor browser bundle, Retrieved from https://www.torproject.org/projects/torbrowser.html.en

Twitter: About us. (n.d.). Retrieved from http://twitter.com/about

Twitter: Wikileaks. (n.d.). Retrieved from http://twitter.com/wikileaks

U.S. Department of Homeland Security. (2010). *Quadrennial homeland security review report.* Washington, DC: U.S. Department of Homeland Security.

U.S. Government. (1980, July 3). *A code of ethics for government—Public Law 96-303*. Retrieved from Isocracytx.net website: http://www.isocracytx.net/hp-org/ethics.html

U.S. Merit Systems Protection Board. (2010). *Whistleblower protections for federal employees.* Washington, DC: U.S. Merit Systems Protection Board.

U.S. Office of Special Councel. (2010, January 18). *Whistleblowing.* Retrieved from http://www.osc.gov/wbdiscposter.htm

U.S. Office of Special Counsel. (2004). *Strategy for reducing persistent backlog of cases should be provided to Congress.* Washington, DC: Government Accountability Office.

U.S. Office of Special Counsel. (n.d.). *About prohibited personnel practices*. Retrieved from http://www.osc.gov/pppwhatare.htm

U.S. Senate. (2002, November 19). *Committee reports—107th Congress (2001–2002) Senate report 107-349*. Retrieved from Library of Congress—Thomas website: http://thomas.loc.gov/cgi-bin/cpquery/0?&&dbname=cp107&&&r_n=sr349.107&&sel=DOC&

U.S. Supreme Court. (2006, October). *Garcetti v. Ceballos*. Retrieved from http://supreme.justia.com/us/547/04-473/

United States Code. (n.d.). *6 U.S.C. § 463: U.S. Code—Section 463: Requirement to comply with laws protecting equal employment opportunity and providing whistleblower protections*. Retrieved from Findlaw website: http://codes.lp.findlaw.com/uscode/6/1/VIII/H/463

United States Code. (n.d.). *Title 5 Part III Subpart A Chapter 23 § 2302. Prohibited personnel practices*. Retrieved from http://www.law.cornell.edu/uscode/5/2302.html

United States Court of Appeals, Ninth Circuit. (2007, 26 December). *United States Court of Appeals: Marable v. Nicthman*. Retrieved from Findlaw.com website: http://caselaw.findlaw.com/us-9th-circuit/1255034.html

United States Court of Appeals, Tenth Circuit. (2008, December 03). *United States Court of Appeals, Tenth Circuit:Thomas v City of Blanchard*. Retrieved from Findlaw website: http://caselaw.findlaw.com/us-10th-circuit/1164922.html

Ushahidi: About us. (n.d.). Retrieved from http://www.ushahidi.com/about

Uys, T. (2011, October 13). *Challenges in the sociology of business ethics: Researching whistleblowing*. Retrieved from African Journal of Busines Ethics website: http://www.ajobe.org/article.asp?issn=1817-7417;year=2011;volume=5;issue=1;spage=50;epage=57;aulast=Uys

Van Leuven, L. (2009). *Optimizing citizen engagement during emergencies through use of web 2.0 technologies* (master’s thesis). Naval Postgraduate School, Monterey, CA.

Vandekerckhove, W. (2010). Risky rescues and the duty the blow the whistle. *Journal of Business Ethics,* 365–380.

Verschoor, C. C. (2010, May). We need more whistleblowers. *Strategic Finance*, 15–16, 61.

Weeks, B. (2010, February 11). *The changing face of journalism*. Retrieved from Kansas News Media website: http://wichitaliberty.org/kansas-news-media/the-changing-face-of-journalism/

Welch, E. (2003). Proceedings of the 36th Annual Hawaii International Conference on System Sciences: *Internet use, transparency, and interactivity effects on trust in government*. (p. 7). Washington, DC: IEEE Computer Society.

West, D. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review*, 15–27.

Whistleblowing CEE Project. (n.d.). *What is whistleblowing*. Retrieved from http://www.whistleblowing-cee.org/about_whistleblowing/#download

Wikileaks: About us. (n.d.). Retrieved from http://www.wikileaks.org/media/about.html

WiTopia. (2012). https://www.witopia.net/

xerobank. (n.d.). https://xerobank.com/

Zarsky, T. Z. (2004). *Thinking outside the box: Considering transparency, anonymity, and pseudonymity as overal soultions to the problems of information privacy in the internet society*. Miami: University of Miami.

Zetter, K. (2010, July 14). *NSA executive leaked after official reporting process failed him*. Retrieved from Wired Threat Level website: http://www.wired.com/threatlevel/2010/07/thomas-drake/

Zimbardo, P. (2007). *The lucifer effect.* New York: Random House.

Zusman, M. (2009, February 19). *Moxie marlinspike un-masks tor users*. Retrieved from Intrepid U.S. Group, Insight: http://intrepidusgroup.com/insight/2009/02/moxie-marlinspike-un-masks-tor-users/

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California